CORPORACIÓN FINANCIERA NACIONAL

CONTRATO DE PRESTACIÓN DE SERVICIOS No. 005-2020
"RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS"

(RI-INV-CFNGYE-009-2019)

Comparecen a la celebración del presente contrato, por una parte la **CORPORACIÓN FINANCIERA NACIONAL B.P,** representada por la Ing. Grace Ivonne Rodríguez Barcos, en su calidad de Gerente Administrativa, quien actúa debidamente autorizada por la delegación otorgada por el Gerente General de la Institución, contenida en Resolución No. **CFN-B.P.-GG-2019-0041-R** de fecha 22 de abril de 2019, a quien en adelante se le denominará la **CONTRATANTE** o la CFN; y,

Por otra parte la compañía **ITSEGUINFO CIA. LTDA.,** representada por la Señor Carlos Jumbo Guaycha, en su calidad de Gerente General , a quien en adelante se la denominará la **CONTRATISTA.** Las partes se obligan en virtud del presente contrato, al tenor de las siguientes cláusulas:

Cláusula Primera.- INTERPRETACIÓN DEL CONTRATO

1.1. Los términos del contrato se interpretarán en su sentido literal, a fin de revelar claramente la intención de los contratantes. En todo caso su interpretación sigue las siguientes normas:

a. Cuando los términos están definidos en la normativa del Sistema Nacional de Contratación Pública, Reglamento Interno de Contrataciones por Giro Específico de Negocio de la Corporación Financiera Nacional B.P. o en este contrato, se atenderá su tenor literal.
b. Si no están definidos se estará a lo dispuesto en el contrato en su sentido natural y obvio, de conformidad con el objeto contractual y la intención de los contratantes. De existir contradicciones entre el contrato y los documentos del mismo, prevalecerán las normas del contrato.
c. El contexto servirá para ilustrar el sentido de cada una de sus partes, de manera que haya entre todas ellas la debida correspondencia y armonía.
d. En su falta o insuficiencia se aplicarán las normas contenidas en el Título XIII del Libro IV de la Codificación del Código Civil, "De la Interpretación de los Contratos".

1.2. Definiciones: En el presente contrato, los siguientes términos serán interpretados de la manera que se indica a continuación:

a. "Adjudicatario", es el oferente a quien la entidad contratante le adjudica el contrato.

b. "Contratista", es el oferente adjudicatario.

c. "Contratante" "Entidad Contratante", es la entidad pública que ha tramitado el procedimiento del cual surge o se deriva el presente contrato.

d. "LOSNCP", Ley Orgánica del Sistema Nacional de Contratación Pública.

e. "RGLOSNCP", Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Púbica.

f. "RICGNCFNBP", Reglamento Interno de Contrataciones por Giro Específico de Negocio de la Corporación Financiera Nacional B.P.

g. "Oferente", es la persona natural o jurídica, asociación o consorcio que presenta una "oferta", en atención al procedimiento de contratación.

h. "Oferta", es la propuesta para contratar, ceñida al pliego, presentada por el oferente a través de la cual se obliga, en caso de ser adjudicada, a suscribir el contrato y a la provisión de bienes o prestación de servicios.

i. "SERCOP", Servicio Nacional de Contratación Pública.

CORPORACIÓN FINANCIERA NACIONAL

Cláusula Segunda.- ANTECEDENTES

2.1. De conformidad con lo establecido en el artículo 8 del Reglamento Interno de Contratación de la CFN B.P., en concordancia con los artículos 22 de la Ley Orgánica del Sistema Nacional de Contratación Pública –LOSNCP-, y 25 y 26 de su Reglamento General -RGLOSNCP-, el Plan Anual de Contrataciones de la CORPORACIÓN FINANCIERA NACIONAL B.P., contempla la contratación de la **"RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS"**

2.2. Mediante documento 2019-GPCR1-00499, de fecha 05 de diciembre de 2019, la Subgerencia de Operaciones Financieras, certificó que con cargo a la partida presupuestaria Nro. 45071502 denominada **"MANTENIMIENTO EQUIPOS DE COMPUTACIÓN"**, existen los fondos suficientes para la contratación de la **"RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS"**

2.3. Previo a informes y estudios respectivos, la delegada de la máxima autoridad de la CONTRATANTE, mediante sumilla inserta en el memorando Nro. CFN-BP.-SCOP-2019-0743-M de fecha 05 de diciembre de 2019, autorizó el inicio del proceso de manifestación de interés para la contratación de la **RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS**, de conformidad con lo previsto en el Capítulo II "Del procedimiento de Invitación y Selección para la ejecución de obras, adquisición de bienes y prestación de servicios", Sección I "Conformación de la lista de interés de proveedores de obras, bienes o servicios" del Reglamento Interno de Contrataciones de la Corporación Financiera Nacional B.P., con la finalidad de identificar las micro, pequeñas y medianas empresas que tengan capacidad para la ejecución del referido proyecto.

2.4. Una vez finalizado el proceso de Manifestación de Interés Nro. **RI-MIN-CFNGYE-009-2019**, con fundamento en lo establecido en el Capítulo II, Sección II, artículo 59, del Reglamento Interno de Contrataciones de la Corporación Financiera Nacional B.P, la Abg. Andrea Mera Servigón, Subgerente de Compras Públicas, solicitó autorizar el inicio del proceso de contratación para la **RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS**, con un presupuesto de USD$45,927.04 (Cuarenta y cinco mil novecientos veintisiete 04/100 Dólares Americanos) más IVA, y con un plazo de 733 días contados a partir de la suscripción del contrato.

2.5. Con fecha 18 de diciembre de 2019, a través del Sistema de Gestión Documental Quipux, mediante comentario inserto al Memorando Nro.**CFN-B.P.-SCOP-2019-0781-M**, se autorizó el proceso de Invitación y Selección Nro. **RI-INV-CFNGYE-009-2019** para la contratación de la **RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS**, con un presupuesto referencial de USD$45,927.04 (Cuarenta y Cinco Mil Novecientos Veintisiete 04/100 Dólares Americanos) más IVA, y con un plazo de 733 días contados a partir de la suscripción del contrato, invitando a participar al proveedor **ITSEGUINFO CIA. LTDA**, con **RUC 1792199387001**;

2.6. Luego del proceso correspondiente, mediante Resolución **No. CFN-B.P.-GEAD-2019-0203-R** de fecha 18 de diciembre de 2019, la Ing. Grace Rodríguez Barcos, en su calidad de delegada de la máxima autoridad de la Contratante, resolvió aprobar el pliego precontractual y disponer el inicio del proceso de **Invitación y Selección Nro. RI-INV-CFNGYE-009-2019**, para la **RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS**, de acuerdo a lo establecido en el Reglamento Interno de Contrataciones de la CFN B.P. Capítulo II, Sección II, artículo 58 y siguientes, la Ley Orgánica del Sistema Nacional de Contratación Pública y su Reglamento General.

2.7. De conformidad con lo establecido en el Capítulo II "Del procedimiento de Invitación y Selección para la ejecución de obras, adquisición de bienes o prestación de servicios", Sección II "Del Procedimiento de Invitación y Selección", artículo 64 del Reglamento Interno de Contrataciones de la Corporación Financiera Nacional B.P., la delegada de la máxima autoridad de la CONTRATANTE, mediante Resolución Nro. **CFN-B.P.-GEAD-2020-0007-R**, de fecha 24 de enero de 2020, adjudicó el contrato para la **"RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS"** al proveedor **ITSEGUINFO CIA. LTDA**, con **RUC 1792199387001**, por un valor de USD$45.927.04 (Cuarenta y Cinco Mil Novecientos Veintisiete 04/100Dólares de los Estados Unidos de América).

2.8. La presente contratación cuenta con los recursos presupuestarios suficientes, conforme consta en el documento 2020-GPCR1-00075, de fecha 23 de enero de 2019, mediante el cual la Subgerencia de Operaciones Financieras, actualiza la certificación contenida en el documento Nro. **2019-GPCR1-00499**, en la que certifica que existen los fondos suficientes para la contratación de la **"RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR**

DOS AÑOS", en la partida presupuestaria Nro. 45071502 denominada **"MANTENIMIENTO EQUIPOS DE COMPUTACIÓN"**.

Cláusula Tercera.- DOCUMENTOS DEL CONTRATO

Forman parte integrante del contrato los siguientes documentos:

a) El pliego (Condiciones Particulares del Pliego CPP y Condiciones Generales del Pliego CGP de Invitación y Selección) publicados en la página web de la CFN B.P. (https://www.cfn.fin.ec/cfn.-contrata/, incluyendo las especificaciones técnicas o términos de referencia del servicio contratado.

b) La certificación de Fondos 2020-GPCR1-00075, de fecha 23 de enero de 2020 emitida por el Econ. Justo Estévez Estrella, Subgerencia de Operaciones Financiera, que acredita la existencia de la partida presupuestaria y disponibilidad de recursos, para el cumplimiento de las obligaciones derivadas del contrato.

c) La oferta presentada por la CONTRATISTA, con todos los documentos que la conforman.

d) La Resolución de Adjudicación Nro. **CFN-B.P.-GEAD-2019-0007-R**, de fecha 24 de enero de 2020.

e) Nombramiento, copias de la cédula de ciudadanía y del certificado de votación del representa legal de la Contratista.

Cláusula Cuarta.- OBJETO DEL CONTRATO

4.1. La CONTRATISTA se obliga para con la CONTRATANTE a la ejecución del contrato para la **"RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS"** a entera satisfacción de la contratante, según las características y especificaciones técnicas o términos de referencia constantes en la oferta, que se agrega y forma parte integrante de este contrato, en los que se contemplan lo siguiente:

- Mil ciento veinte y ocho (1128) del módulo de antivirus
- Novecientas cuarenta y ocho (948) licencias del módulo de cifrado de información (590 cifrado Estándar y 358 cifrado Pro)

4.1.2. OBJETIVOS DE LA CONTRATACIÓN

Los objetivos de la contratación son:

• Contar con una herramienta de seguridad y protección contra ataques de virus informáticos y otras amenazas de software malicioso (malware).

• Salvaguardar la información institucional de accesos no autorizados, mediante el cifrado de información.

4.2. ALCANCE

La presente contratación tiene como alcance contar con la renovación de mil ciento veinte y ocho (1128) licencias del módulo de antivirus y novecientas cuarenta y ocho (948) licencias del módulo de cifrado de información de la Suite de Seguridad ESET Endpoint Protection Advanced con los que cuenta la institución, por el período de dos años, para todos los equipos de computación (escritorio y portátiles) y servidores de la CFN B.P., a nivel nacional, adicionalmente también se va a instalar en las computadoras institucionales, el módulo ESET Enterprise Inspector, que es una solución complementaria de seguridad para detectar cambios en el sistema operativo, que podrían convertirse en ataques de virus informáticos en la red.

4.3. METODOLOGÍA DE TRABAJO

La metodología de trabajo, contempla los siguientes aspectos:

4.3.1. La contratista deberá proporcionar el servicio de renovación de las licencias de los módulos de antivirus y cifrado de información, y la instalación y configuración del End Point Advanced, de la Suite de Seguridad ESET Endpoint Protection Advanced con los que cuenta la institución, durante la vigencia del contrato.

4.3.2. La contratista deberá emitir un informe técnico, que certifique la renovación, instalación y configuración de las licencias de la Suite de Seguridad ESET Endpoint Protection Advanced, a la última versión vigente del software.

4.3.3. El soporte técnico deberá estar vigente durante la ejecución del contrato y deberá tener las siguientes características mínimas:

- Disponibilidad horario laboral bajo la modalidad 9x5.
- Atención vía telefónica, correo electrónico o asistencia remota para análisis de daños y posible solución.
- Para atención presencial en el sitio del incidente cuando se lo requiera por parte de la contratante:
  Prioridad Alta, máximo 1 hora
  Prioridad media, máximo 2 horas
  Prioridad baja, máximo 4 horas.

➢ **Requerimientos por Gestión de Riesgo Operativo – SB:**

De conformidad con los requerimientos por Gestión de Riesgos Operativo conforme a las disposiciones de la Superintendencia de Bancos, la contratista durante la ejecución del contrato deberá cumplir con lo establecido en los acuerdos que se detallan a continuación:

A. Acuerdo de nivel de servicio (SLA)

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral b,, i: Niveles mínimos de calidad del servicio acordado, de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, la contratista deberá cumplir con lo establecido en el "ACUERDO DE NIVEL DE SERVICIO", de acuerdo a lo presentado en su oferta.

En el acuerdo de nivel de servicio se incluye como mínimo lo siguiente:

- Acuerdo de Nivel de Servicio (SLA)
- Periodo de Evaluación: mensual
- Disponibilidad mínima mensual del servicio 99,6%

1. Tiempos de respuesta y reparación para el servicio

- El servicio de soporte técnico deberá ser en modalidad de 8x5 (8 horas al día, 5 días a la semana) en días y horas laborables.

- Los tiempos de indisponibilidad del servicio serán contabilizados desde el momento de notificación del incidente al Centro de Atención del contratista y en caso de problema, desde la llamada al contacto del escalamiento del contratista.

2. Prioridad de Servicio de Soporte:

Los servicios de soporte, deberán ejecutarse bajo el esquema de atención y por el tipo de prioridad o severidad:

La prioridad o severidad será definida por la CFN B.P de acuerdo al conocimiento que tiene del impacto hacia el negocio, y conforme al siguiente esquema:

3. **Prioridad Alta: De carácter "Urgente".**

Cuando el servicio se encuentre "caído" o el impacto sobre la operación es crítico lo cual impacta a la disponibilidad. La contratista y la contratante se comprometen a dedicar recursos de tiempo completo, de acuerdo al nivel adquirido para resolver la situación.

El tiempo máximo transcurrido desde el reporte del incidente hasta su atención es de **1 hora** y de solución en **4 horas**.

4. **Prioridad Media: De carácter "Importante".**

Cuando se tenga una degradación en el servicio o aspectos importantes de la operación se ven afectados negativamente por el desempeño inadecuado de los servicios; pero esta aún no afecta la disponibilidad del servicio. La contratista y la contratante se comprometen a dedicar recursos de tiempo completo, de acuerdo al nivel adquirido para resolver la situación.

El tiempo máximo transcurrido desde el reporte del incidente hasta su atención es de **2 horas** y de solución en **8 horas**.

5. **Prioridad Baja:**

Cuando no hay afectación a la disponibilidad del servicio o no hay degradación del servicio, pero se requiere ejecutar un mantenimiento, se requiere información o asistencia para instalación o configuración. La contratista y la contratante se comprometen a brindar los recursos necesarios para entregar la información del soporte o requerimiento solicitado.

El tiempo máximo transcurrido desde el reporte del incidente hasta su atención es de **4 horas** y de solución en **16 horas**.

Prioridad	Medio de Comunicación	Tiempo de Atención y Solución	Entregable
ALTA	Vía telefónica y/o correo electrónico al contacto indicado por el proveedor para constancia y registro respectivo	1 hora para la atención y 4 para la solución	Informe de trabajos realizados asociados al ticket de atención respectivo.
MEDIA	Vía telefónica y/o correo electrónico al contacto indicado por el proveedor para constancia y registro respectivo	2 horas para la atención y 8 para la solución	Informe de trabajos realizados asociados al ticket de atención respectivo.
BAJA	Vía telefónica y/o correo electrónico al contacto indicado por el proveedor para constancia y registro respectivo	4 horas para la atención y 16 para la solución	Informe de trabajos realizados asociados al ticket de atención respectivo.

6. **Nivel de escalamiento para los incidentes:**

- **Primer nivel**: Mediante atención telefónica o correo electrónico; la CFN B.P. realizará el seguimiento respectivo del caso reportado.
- **Segundo nivel:** La contratista deberá proporcionar soporte local o remoto en sitio; para ello, deberá contar con personal especializado para clarificar, aislar y resolver problemas relacionados con la infraestructura objeto del proceso de contratación.
- **Tercer nivel**: Cuando sea requerido, la Contratista, escalará el caso al siguiente nivel de soporte es decir al fabricante (ESET), teniendo que proporcionar a la Contratante el número de caso asignado para efectos de seguimiento, y será obligación de la contratista mantener informado del estado/progreso en la resolución del caso, a los técnicos de la Contratante.

7. **Tiempo de resolución:**

El tiempo máximo para atención y solución, van como se menciona en el numeral 2 *"Prioridad del servicio de soporte"*.

CORPORACIÓN FINANCIERA NACIONAL

8. **Penalizaciones:**

Las multas se impondrán en caso de existir incumplimiento en el Acuerdo de Nivel de Servicio (SLA), en los tiempos de atención o resolución de incidentes, definidos en el mismo, en otros casos aplicará los términos definidos en el contrato. El detalle se encuentra en el apartado que corresponde a multas.

- **Acuerdo de Transferencia de Conocimientos**

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral b., v: Transferencia del conocimiento del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio esencialmente en aquellos definidos como críticos", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, la contratista deberá cumplir con lo establecido en el **"ACUERDO DE TRANSFERENCIA DE CONOCIMIENTOS"**, de acuerdo a lo presentado en su oferta.

En el acuerdo de transferencia de conocimientos se incluye como mínimo lo siguiente:

- El personal técnico designado por la contratista, deberá brindar la respectiva transferencia de conocimientos donde se exponga la administración, operación, y monitoreo de la solución instalada en CFN B.P.
- La transferencia de conocimientos se la realizará, a los tres meses de iniciada la vigencia del contrato, por una sola vez, a menos que se libere una nueva versión de la herramienta, en cuyo caso se tendrá que realizar una nueva capacitación por cada versión liberada durante la ejecución del contrato, en la fecha y hora que la CFN B.P. lo requiera; estas capacitación no tendrá ningún costo adicional para la Contratante.
- La transferencia de conocimientos se deberá realizar como mínimo a 4 funcionarios de la CFN B.P. en las instalaciones de la CFN B.P. en la ciudad de Quito y deberá tener un mínimo de 2 horas, deberá incluir el material didáctico y físico para los participantes.
- La transferencia de conocimientos debe ser realizada por el personal capacitado y calificado, presentado en la oferta, de manera presencial.
- La transferencia de conocimientos debe ser coordinada por el administrador del contrato.
- Como productos entregables de la fase de transferencia de conocimientos, la Contratista deberá entregar acta de transferencia de conocimientos, certificados de participación, el mismo que debe contener: tema, número de horas de duración, nombre del instructor con su firma y sello de la contratista y deberá ser entregado, máximo a los 3 días posteriores a la realización de dicha trasferencia.
- La transferencia de conocimientos, no tendrá costo adicional para la CFN B.P.

- **Acuerdo de confidencialidad de la información y datos**

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGOS OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTÍCULO 14, b., vi. "Confidencialidad de la información y datos", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, la Contratista deberá cumplir con lo establecido en el **"ACUERDO DE CONFIDENCIALIDAD DE INFORMACIÓN Y DATOS"**, de acuerdo a lo presentado en su oferta.

En el acuerdo de confidencialidad de la información y datos se incluye como mínimo lo siguiente:

- Será responsabilidad de la Contratista el guardar absoluta reserva sobre la información y las aplicaciones de propiedad de la CFN B.P. que acceda o le sea confiada en virtud de la ejecución, desarrollo o cumplimiento del contrato, inclusive la información que pueda ser expuesta debido a vulnerabilidades en los sistemas de la CFN B.P.

- La inobservancia de lo manifestado dará lugar a que la Corporación Financiera Nacional B.P. ejerza las acciones legales, civiles y penales correspondientes determinadas en el Código Orgánico Integral Penal.

  La contratista será responsable del cumplimiento del acuerdo por parte del personal que empleare para la ejecución del contrato.

- La contratista guardará absoluta confidencialidad sobre la información en caso de que llegara a conocer información confidencial de la institución, no pudiendo reproducirla, generarla o difundirla en ninguna forma después de la suscripción del contrato.

- La contratista no podrá asistir a entrevistas o sustentar el caso ante ningún medio de comunicación, a menos que reciba autorización escrita del representante legal de la CFN B.P., caso en el cual deberá preparar su exposición conjuntamente con la máxima autoridad, debiendo sustentar la posición institucional de la CFN B.P. con prudencia, evitando el menoscabo de la imagen institucional.

- La contratista se compromete a que el personal a su cargo guarde el mismo nivel de confidencialidad sobre la información recibida con el mismo grado de cautela con el que protege su propia información.

- La contratista y sus técnicos se comprometen a firmar un acuerdo de confidencialidad previo a la suscripción del contrato.

➢ **Acuerdo de derechos de propiedad intelectual del conocimiento, productos, datos e información**

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral b., vii: Derechos de propiedad intelectual, productos, datos e información, cuando aplique" de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, la Contratista deberá cumplir con lo establecido en el **"ACUERDO DE PROPIEDAD INTELECTUAL"**, de acuerdo a lo presentado en su oferta.

En el acuerdo de propiedad intelectual se incluye como mínimo lo siguiente:

- Los informes, materiales didácticos, código fuente, conocimientos, productos, datos; e, información que, de ser el caso, resulten de la ejecución del contrato serán de propiedad exclusiva de la CFN B.P. y no podrán ser divulgados total o parcialmente por el profesional y/o por los profesionales que participen en la ejecución del contrato.

- La CFN B.P. podrá hacer uso que considere conveniente y sea aplicable, de los informes, materiales didácticos, código fuente, conocimientos, productos, datos; e, información que se generen durante la ejecución del contrato, de acuerdo con los intereses institucionales.

- La CFN B.P. podrá realizar el registro en el Servicio Nacional de Derechos Intelectuales (SENADI) cuando lo considere conveniente y sea aplicable, para los informes, materiales didácticos, código fuente, conocimientos, productos, datos; e, información que se generen durante la ejecución del contrato, de acuerdo con los intereses institucionales.

➢ **Acuerdo del equipo de trabajo y administrador/supervisor del contrato en el proveedor**

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE

RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral b., viii: Definición del equipo de contraparte y administrador/supervisor del contrato tanto de la entidad controlada como del proveedor", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, la contratista deberá cumplir con lo establecido en el **"ACUERDO DEL EQUIPO DE TRABAJO Y ADMINISTRADOR/SUPERVISOR DEL CONTRATO"**, de acuerdo a lo presentado en su oferta.

En el acuerdo del equipo de trabajo y administrador/supervisor del contrato se incluye como mínimo las siguientes obligaciones:

- Designar un supervisor de contrato / proyecto por parte de la contratista.
- Definir el equipo de trabajo designado para brindar el servicio.

4.4. INFORMACIÓN QUE DISPONE LA ENTIDAD

La Corporación Financiera Nacional B.P., cuenta con:

- Dos consolas de administración de la Suite de Seguridad ESET para el módulo de antivirus, las mismas que son independientes para Quito y Guayaquil y están divididas para sus regionales (Región 1 y Región 2).

- Una consola centralizada de administración de la Suite de Seguridad ESET para el módulo de cifrado de información en Quito, a la cual se reportan todos los equipos de cómputo que tienen instalado la licencia de este módulo a nivel nacional.

La cantidad de licencias a renovarse por cada módulo es la siguiente:

MODULO	LICENCIAS A RENOVAR
ANTIVIRUS	1128
CIFRADO	948

De las 948 licencias del módulo de cifrado de información, 358 son categoría PRO ya que deberán ser instaladas en equipos portátiles y 590 son categoría estándar para equipos de escritorio, tal como se indica en el siguiente cuadro:

Licencias		Cantidad	Total
Cifrado	Estándar	590	948
	Pro	358	

4.5. PRODUCTOS O SERVICIOS ESPERADOS

Para la renovación de licencias de la Suite de Seguridad ESET Endpoint Protection Advanced, se solicita lo siguiente:

4.5.1. Detalle de los servicios requeridos:

Mantenimiento y Actualización, la contratista deberá notificar y actualizar los módulos de antivirus y cifrado de información con los nuevos parches y releases que sean publicados, además deberá apoyar en sitio al personal técnico de la CFN B.P. en la aplicación de parches, releases y actualizaciones del producto, liberados durante el período de vigencia del contrato, los mismos que se realizarán en horarios de baja afectación y previa coordinación con el administrador de contrato.

La contratista deberá entregar el medio físico de instalación (CD), manuales y documentación digital; y el código necesario para la activación de las licencias en servidores y equipos de usuario final, una vez que se encuentren renovadas las licencias de la Suite de Seguridad ESET Endpoint Protection Advanced.

La contratista se comprometerá a dejar listas y actualizadas, las consolas de administración de los módulos de antivirus y cifrado de información, con el total de equipos de usuario final conectados a las consolas respectivas.

La contratista será responsable de la actualización de los productos antivirus y de cifrado de información con la última versión estable liberada por el fabricante durante la vigencia del contrato.

La contratista será el responsable de implementar en las consolas de la herramienta, las siguientes opciones para el manejo de dispositivos removibles:

- Bloqueo de dispositivos USB que no son de la Institución,
- Autorización de lectura y escritura para los dispositivos USB institucionales, para lo que se registrará información del dispositivo y podrá ser visualizado en cualquier equipo de usuario final a nivel nacional.

4.5.2. Características de las Licencias de Antivirus y Cifrado de Archivos

Protección a nivel de estaciones de trabajo y servidores.	El producto deberá permitir proteger a los equipos contra código malicioso (malware) tal como: Adware, Backdoor, Badware Alcalinos, Bombas, Bomba fork, Bots, Caballo de Troya, Cookies, Crackers, Cryptovirus, Dialers, Exploit, Hijacker, Hoaxes, Jokes, Keystroke o keyloggers, Leapfrog, Parásito Informático, Pharming, Phishings, Pornware, Rabbit, Riskware, Rootkit, Scumware, Spam, Spyware, Ventanas emergentes/POP-UPS, Virus, Worms (gusanos). Protección contra ataques a la red. Protección proactiva sobre aplicaciones de ofimática (Microsoft, Open office). Ser altamente efectivo y fácil de usar. Ofrecer la capacidad de desplegar y administrar fácilmente los productos en las estaciones de trabajo, de modo que se pueda aplicar la política de seguridad corporativa en forma sencilla sin necesidad de imponer grandes exigencias al personal ni a los recursos del sistema.
Administración Centralizada de la solución.	Soporte para múltiples plataformas, debe funcionar tanto en equipos Windows como Linux, Mac, permitiendo instalarse todos los componentes deseados simultáneamente con el programa de instalación general o eligiendo los componentes individuales Vista general perfecta de la seguridad de la red. Incluir un sensor detector de equipos no autorizados, descubrir todos los equipos de la red que no están protegidos ni administrados y mostrárselos al administrador. Grupos dinámicos y estáticos, asignar clientes a grupos estáticos o dinámicos y establecer los criterios de inclusión para cada grupo dinámico; los clientes designados deben pasar a pertenecer automáticamente al grupo respectivo. Definir las tareas específicas que se deben ejecutar y en qué momento.

	Permitir manejar todas las licencias a través de una sola consola de administración, en forma transparente desde un solo lugar. Crear múltiples cuentas de usuarios y personalizarlas, los privilegios para cada una se podrán personalizar en forma individual. Se podrá usar en muchas ubicaciones distintas y permitir definir políticas corporativas para los administradores locales. Utilizar el estándar de Seguridad de la capa de transporte (TLS) 1.0. También emplear certificados propios creados y distribuidos especialmente para firmar en forma digital y para cifrar las comunicaciones entre los componentes individuales de la solución con el objetivo de identificar a los pares. Limpieza de equipos terminales y servidores de código malicioso y programas inseguros no autorizados instalados en los equipos de cómputo. Además de mostrar los informes a través de la consola basada en la Web, se pueden exportar en formato PDF y guardar en una ubicación predefinida, o enviarse como una notificación por correo electrónico. Protección contra vulnerabilidades: Mejora la detección de las Vulnerabilidades y Exposiciones Comunes (CVE) en los protocolos más utilizados, como SMB, RPC y RDP. Brinda protección contra las vulnerabilidades para las cuales aún no se publicó o desarrolló la revisión necesaria. Protección ante botnets: Protege ante las infiltraciones por malware de tipo botnet, previniendo el envío de spam y evitando que se lleven a cabo ataques de red desde los endpoints. Desinstalación de soluciones de seguridad: la solución deberá ser capaz de desinstalar la solución que se encuentra instalada actualmente. Instalación/ desinstalación de Software de terceros: La consola deberá tener la posibilidad de desinstalar software instalado en los equipos. Deberá contar con la posibilidad de sincronizarse con el Active Directory. Debe permitir generar grupos de clientes dinámicos (paramétricos) y grupos estáticos. La consola de gestión debe mostrar la lista de servidores y estaciones que tienen el antivirus instalado. Debe ser capaz de instalarse en un entorno de clúster y ante la caída de un servidor levantar el otro automáticamente sin pérdida alguna de datos ni de disponibilidad. Que al ejecutar un análisis en un endpoint el consumo de memoria del servidor sea menor a los 23Mb.
Protección para Plataformas	El Producto deberá proteger las siguientes plataformas:

Windows, Linux y Mac OS	Sistemas operativos Microsoft Windows XP SP3, con disco de 300 GB, RAM de 512 MB con red. Microsoft Windows Vista SP1 Microsoft Windows 7, Microsoft Windows 8, Windows 10. Versión para servidores: Microsoft Windows Server 2016, 2012R2, 2012, 2008R2, 2008, 2003. Microsoft Windows Server Core 2012R2, 2012, 2008R2, 2008 Core. Microsoft Small Business Server 2011, 2008, 2003R2, 2003. Linux Mac OS
Protección en tiempo real	El producto deberá contar con protección en tiempo real a través de tecnología denominada como Heurística Avanzada, además de su protección reactiva en base a firmas, lo cual permita detectar y detener todo tipo de código o software malicioso alojado en unidades de discos duros fijos o removibles.
Filtrado de correo electrónico	El producto deberá examinar con eficiencia los buzones de entrada de los usuarios finales en busca de spam, ataques de phishing y mensajes de correo electrónico no solicitados. Las listas blanca y negra, así como el aprendizaje automático, se pueden configurar en forma separada para cada cliente o grupo. El soporte nativo para Microsoft Outlook mejora la protección (POP3, IMAP, MAPI, HTTP) ante amenazas en línea sin generarle trabajo adicional.
Filtrado de SPAM en correo electrónico.	El producto deberá ofrecer un módulo antispam que permita realizar análisis en tiempo real.
Filtrado de Navegación	Deberá tener filtrado de navegación realizando la búsqueda en tiempo real de códigos maliciosos en tráfico HTTP y HTTPS, debiendo filtrar el código malicioso antes de que se escriba en las carpetas temporales del disco duro. Ofrecer una alta velocidad de exploración con un mínimo impacto en el sistema, lo que lo ayudará a preservar el rendimiento de los equipos corporativos, a mantenerlos funcionando sin problemas y a extender la vida y la usabilidad del hardware.
Protección Proactiva	El Producto deberá contar con protección proactiva y reactiva para impedir modificaciones al sistema (cambios en el registro). Proteger la infraestructura crítica corporativa durante el período crucial posterior a los brotes de malware. La tecnología de heurística avanzada deberá proteger los endpoints e impedir que los códigos maliciosos logren abrirse paso en la red.
Tecnología de heurística avanzada	Utilizándola para la detección heurística de malware para proteger los sistemas corporativos de las amenazas conocidas y emergentes, a la vez que mantener los falsos positivos en un mínimo. Que permita la optimización inteligente mediante configuración predefinida, que proporcione la combinación más eficiente de la protección del sistema y la velocidad de la exploración.
Instalación por componentes	La protección de correo electrónico deberá tener la posibilidad de instalarse por componentes, puede elegir los componentes a añadir o eliminar.

Tecnología de Emulación	La solución propuesta deberá contar con una tecnología que someta al código malicioso a una monitorización activa, mientras se ejecuta en un entorno protegido (también conocido como "sandbox"). Basándose en el comportamiento del código, esta tecnología determinará si la muestra dada representa una amenaza e inmediatamente marca o elimina todas las aplicaciones dañinas.
Heurística avanzada en medios extraíbles y ejecución de archivos	Que emule el código en un entorno virtual y evalué su comportamiento antes de que se permita la ejecución del código desde un medio extraíble.
Bloqueo de Exploits	La solución propuesta deberá contar con un sistema de bloqueo de Exploits y debe estar dirigido al problema de vulnerabilidades 0-day (día cero) para las aplicaciones más comunes, como navegadores Web, Java, lectores de PDF y herramientas de Microsoft Office. Debe utilizar una tecnología completamente diferente a las que solo se basan en la detección de archivos maliciosos, y así lograr estar un paso más cerca de los atacantes.
Explorar secuencias de datos alternativas ADS	Que permita la exploración de las secuencias de datos alternativas usadas por el sistema de archivos NTFS, constituyendo asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración.
Tecnología de Análisis de código	La solución propuesta deberá contar con una tecnología de detección al analizar archivos para buscar semejanzas con muestras de códigos maliciosos conocidos antes de que se desarrolle la firma de virus. Basándose en el comportamiento del código, esta tecnología determinará si la muestra dada representa una amenaza e inmediatamente marca o elimina todas las aplicaciones dañinas.
Tamaño del instalador	El tamaño del instalador de la herramienta antivirus, no deberá exceder de 70Mb.
Consumo de recursos de Memoria del Endpoint	Que el producto utilice menos de 120Mb de memoria RAM cuando este inactivo el sistema. Que el producto utilice menos de 250Mb cuando se ejecute un análisis completo.
Exclusión de archivos del análisis en tiempo real	El producto deberá contar con la opción para realizar exclusiones de archivos del análisis en tiempo real.
Control de acceso web	El producto deberá contar con un control de acceso web, con categorías para definir qué sitios pueden ser accedidos o no dentro de la red. Limitar el acceso a los sitios Web por categoría y por grupo de usuarios para lograr una eficaz aplicación de las políticas corporativas cuyo objetivo es maximizar el cumplimiento de directivas de seguridad y la productividad de los empleados.
Firewall inteligente	Impedir el acceso no autorizado a la red corporativa. Ofrecer una fácil instalación, gran capacidad de personalización de reglas y un modo de aprendizaje inteligente para crear reglas de firewall automáticamente basándose en el tráfico de red observado. Combinar perfiles personalizados de firewall con zonas de redes de confianza.
Análisis manual de búsqueda de códigos maliciosos.	El producto deberá contar con la opción de correr un análisis manual de búsqueda de códigos maliciosos. Ofrecer detección avanzada de

	malware furtivo mediante la exploración minuciosa del contenido de los protocolos seguros HTTPS y POP3S, así como de los archivos comprimidos.
Control de Dispositivos	El producto debe contar con un control de dispositivos que permita bloquear unidades de CD/DVD, dispositivos de almacenamiento masivo, dispositivos de comunicación USB (incluidos los módems), impresoras USB, Dispositivos Bluetooth, lectores de memorias, entre otros.; además de permitir agregar permisos por usuarios y crear reglas para permitir o denegar el acceso a estos dispositivos. Que los bloqueos a dispositivos puedan realizarse por marca, modelo, número de serie o usuario.
Exclusión de archivos	El producto deberá contar con la opción de realizar exclusiones de archivos del análisis del motor por demanda.
Análisis Programados	El producto y la consola de administración remota deberán permitir realizar análisis programados (bajo demanda) de los discos duros locales de equipos de cómputo. Esta programación se podrá configurar en forma diaria, semanal, mensual.
Cortafuegos de escritorio	El producto deberá contar con un cortafuegos de escritorio (Firewall Personal) que cuenta con un filtrado dinámico de paquetes que provea de monitoreo y filtrado de trafico de Red, y tenga total protección para IPv4 e IPv6 y con la opción de agregar reglas y servicios al cortafuego en forma autónoma y centralizada. Debe poseer distintos modos del módulo de firewall entre los cuales debe tener uno que permita aprender la conducta del usuario generando las reglas permisivas automáticamente. Esta solución no deberá provocar interrupciones con el Firewall Perimetral de la Institución.
HIPS (Host-based Intrusion Detection	El producto deberá contar con HIPS (Host-based Intrusion Detection) que proteja su sistema de malware o de cualquier actividad no deseada tratando de afectar negativamente la seguridad de los equipos de cómputo de la CFN B.P. Generar reglas de permiso o denegación sobre aplicaciones cuando estas: depuren otra aplicación, intercepten sucesos desde otra aplicación, intente finalizar o suspender otra aplicación, iniciar una nueva aplicación, o modificar el estado de otra aplicación Generar reglas sobre aplicaciones que intenten realizar las siguientes acciones sobre entradas del registro del sistema: Modificar la configuración del inicio, eliminar entradas del registro, volver a nombrar claves de registro, modificar el registro. Generar reglas sobre archivos que permitan o bloqueen la eliminación, la escritura, el acceso directo al disco, instalar un enlace global o cargar un controlador.

Rollback de base de firmas	El producto antivirus deberá permitir efectuar un Rollback de base de firmas.
Actualizaciones	Que las actualizaciones de base de firmas y componentes ocupen en promedio no más de 0,5Mb diarios y sean programables con intervalos amplios de tiempo.
Actualización a través del servidor de la solución de todas las estaciones protegidas	La consola de administración deberá permitir actualizar a través del servidor de la solución a todas las estaciones protegidas con la posibilidad de tener redundancia de servidores de actualización en forma automáticas (Fail-over).
La actualización de la base de datos de firmas de códigos maliciosos deberá ser incremental, ahorrando de esta manera ancho de banda en su despliegue	Las actualizaciones de las bases de datos de firmas de códigos maliciosos del producto antivirus deberán ser incrementales, evitando de esta manera el ancho de banda en su despliegue.
Opción de apagado luego de escaneo.	La herramienta antivirus debe permitir el apagado luego de la exploración o Repetición de las exploraciones programadas activadas por el usuario. Esto con el objetivo de ayudar a extender la vida útil del hardware y ahorrar energía y optimizar recursos.
Programación y actualizaciones diferidas.	La herramienta antivirus debe contar con una selección opcional para la recepción de actualizaciones provenientes de servidores especiales con 12 horas de retraso para brindar tiempo a los administradores del sistema para evaluar el impacto en su red y asegurar una migración organizada.
Reportes	La consola de administración deberá contar con un mínimo de 36 opciones de reportes gerenciales detallados con información de configuraciones, actualizaciones de los productos, alertas, estadísticas, etc., las cuales pueden ser exportadas a archivos csv y/o html. Deberá permitir generar reportes gráficos tipo barra, pastel, etc., para una vista rápida de la situación del producto.
Alerta en consola y notificación vía correo electrónico y SNMP	El producto deberá permitir que las acciones de notificación incluyan correo electrónico, SNMP, y entradas de registro.
Compatibilidad con la estructura organizacional del Directorio Activo de servidores Windows para la Instalación del producto	La consola de administración deberá permitir la detección de clientes no registrados sincronizando la estructura del grupo a través de Active Directory.
Análisis de aplicaciones y procesos	Debe permitir clasificar las aplicaciones en al menos 3 grupos según sus características y poder configurar el motor antivirus para que las analice o no. Debe otorgar una puntuación a los procesos en ejecución del sistema para medir su nivel de riesgo.
Análisis de procesos	Deberá poseer una herramienta integrada para ver los procesos en ejecución, los servicios, las conexiones establecidas, claves de registro

	importantes, programas instalados, actualizaciones de sistema operativo instaladas, logs del equipo, drivers instalados, tareas programadas del sistema, archivo hosts, system.ini y win.ini.
Análisis de archivo comprimidos	El producto deberá detectar virus en archivos compactados, sin importar el número de niveles de compresión, en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros.
Gestión de Políticas	La consola de administración deberá definir y hacer cumplir consistentemente las políticas a lo largo de la red. El Administrador de Políticas facilitará la importación/exportación, para permitir la aplicación y combinación de las políticas de diversas maneras.
Gestión Multi-plataforma	La consola de administración deberá permitir administrar de forma remota desde una única consola todos los equipos de su red, ejecutando las versiones antivirus en clientes finales y servidores de las diferentes plataformas (Windows, Linux, Mac OS).
Solución para dispositivos móviles (smartphones)	Debe proveer de una solución de seguridad rápida y efectiva para los smartphones corporativos. La herramienta debe tener entre sus características principales las opciones de: Protección contra malware. Función de borrado y bloqueo remoto, Antispam para SMS/MMS., Protección contra desinstalación, Localización de dispositivo por GPS, Auditoría de Seguridad, Bloqueo de llamadas de números desconocidos u ocultos y números no deseados. Que permita definir una lista de contactos permitidos / contactos bloqueados, Cuarentena, Protección contra infiltraciones, Que cuente con administración centralizada, Control de aplicaciones
Seguridad	El producto deberá contener un módulo especial para el análisis de ransomware y amenazas avanzadas así mismo poder realizar informes sobre cada una de estos eventos de seguridad
Cifrado de datos	Debe proveer de una solución de cifrado simple y potente, usando los algoritmos y estándares más avanzados para crear claves impenetrables: Algoritmos y estándares: • AES 256 bit. • AES 128 bit. • SHA 256 bit. • SHA1 160 bit. • RSA 1024 bit. • Triple DES 112 bit. • Blowfish 128 bit. Certificaciones: • FIPS140-2 level 1.
Administrar las claves de cifrado	Debe tener la capacidad de administrar usuarios y estaciones de trabajo independientemente o en relaciones de "muchos a muchos". Permitir el cambio de las políticas de cifrado en forma remota y silenciosa, sin interacción del usuario.
Tipos de cifrado	Permitir administrar fácilmente cualquier usuario o estación de trabajo en forma remota, incluyendo el uso compartido de claves entre clientes en tiempo real.

	• Cifrado del disco completo. • Cifrado de medios extraíbles. • Cifrados de archivos y carpetas. • Cifrados de correo. • Cifrado de texto y portapapeles. • Cifrado de discos virtuales y archivos comprimidos.

4.5.3. Funcionalidades Técnicas Edr y Anti APTs

Consola de administración	La solución de EDR debe poder ser instalada On-Premise y administrar con el mismo agente del EPP los equipos finales.
	Permitir tomar acciones desde la consola on premise sobre el equipo final.
	El agente de EDR se deberá poder instalar de manera remota, al menos por alguno de los siguientes métodos: •Herramienta provista por el propio fabricante. • Línea de comando.
Reportes	La solución de EDR deberá permitir detectar comportamientos sospechosos dentro de los endpoints, en caso de encontrar archivos o procesos extraños, deberá disparar alertas para avisar al administrador.
	La solución de EDR debe proveer un listado de los archivos ejecutables que se ejecutaron dentro de la red.
	La solución de EDR debe proveer un listado de los scripts que se ejecutaron dentro de La red.
	El equipo de seguridad podrá ver qué se vio afectado, dónde y cuándo se realizó el ejecutable, secuencia de comandos o acción específica, y analizar la causa de esto "de vuelta a la raíz".
	Permitir a través de los reportes rastrear los archivos creados en los dispositivos monitoreados, validando su origen, proceso y qué usuario lo creo.
	Los reportes tienen que poder ser editados y ajustados a medida en un archivo excel.
Políticas de seguridad	La solución de EDR deberá permitir la generación de exclusiones utilizando al menos lo siguientes parámetros: • Nombre del archivo • Ubicación del archivo • Equipo • Usuario

	La solución deberá mostrar alertas de seguridad en el equipo del usuario.
	La solución deberá permitir la creación de reglas personalizadas para monitorear determinados comportamientos, por ejemplo: • Modificaciones en llaves del registro del sistema. • Creación de conexiones de red a través de rundll32 • Ejecución de scripts a través de MS Office
	Incluir configuración de filtros múltiples que permitan una tarea automatizada de búsqueda de amenazas y que se puedan ajustar al umbral de detección al entorno específico de la empresa.
	Permitir que el equipo de seguridad pueda configurar y ajustar las reglas de detección que describen las técnicas de ataque al entorno específico de la organización.
	Poder configurar la misma para detectar violaciones de las políticas de la organización sobre el uso de software específico como aplicaciones torrent, almacenamiento en la nube (por ejemplo, Dropbox), navegación Tor, inicio de servidores propios y otro software no deseado.
	Si se identifican amenazas la herramienta deberá incluir un módulo en respuesta a incidentes rápido, que permita bloquear con hash.
	Los procesos se podrán eliminar y poner en cuarentena, y las máquinas seleccionadas se tendrán que aislar o apagar de forma remota.
Análisis forense	La solución de EDR deberá permitir realizar análisis forense y análisis de causa raíz para determinar todo el ciclo de vida de un proceso dentro de la red.
	Incluir todo el ciclo de vida del ataque: análisis desde su detección, cuándo, en qué archivo, el archivo que se ejecutó, el proceso realizado, y los cambios que generó en el sistema.
Análisis de amenazas	La solución de EDR deberá validar la reputación de un archivo o proceso utilizando tecnologías basadas en la nube.
	Para cada alerta generada la solución de EDR deberá indicar en cuantos equipos fue vista esa alerta, a que podría deberse, y cuáles son las posibles acciones a tomar.
	La solución de EDR deberá tener la posibilidad de detener un proceso sospechoso o bien enviarlo para que sea analizado por los administradores.
	La solución de EDR deberá permitir el bloqueo de archivos a través de hash
	Si un usuario activa múltiples alarmas, deberá la herramienta validar su actividad y bloquear si es necesario sus modificaciones.
	El EDR debe identificar fácilmente los elementos débiles y ordenando a los endpoints por el número de alarmas únicas activadas.
	Permitirá aplicar filtros a los datos que se clasifican según la popularidad o la reputación de los archivos, la firma digital, el comportamiento y la información contextual, cualquier actividad maliciosa podrá identificarse e investigarse fácilmente.
	Incluir análisis del contexto del usuario para la generación de alertas reales y disminuir los falsos positivos.

	Para cada alarma activada, se debe incluir un siguiente paso atado a la corrección de dicha vulnerabilidad.
Tecnología	La solución EDR deberá mediante tecnología intuitiva y de análisis de comportamiento (machine learning) deberá permitir a los equipos detectar APTs, archivar menos ataques y prevenir todo tipo de actividad maliciosa.
	La tecnología de seguridad deberá incluir la posibilidad de supervisión de seguridad mejorada, detección de amenazas más sensible, respuesta mejorada y capacidades de remediación automáticas y manuales.
Protección contra malware	Incluir un sistema de recopilación de datos automático.
	Realizar análisis de comportamiento.
	Protección contra embevida, que permita subir las amenazas a la nube y realizar sandbox.
	Contar con un sistema de reputación de archivos embevido, sin necesidad de descargar actualizaciones.
Reputación y caché	Analizar archivos o URLs y comprobar en la memoria caché si es un objeto conocido y clasificarlo en base a su reputación.
Detecciones por ADN	Análisis de definiciones complejas de comportamiento malicioso y características de malware.
	Identificar el malware nunca antes visto que contiene genes que indican un comportamiento malicioso.
	Clasificación de archivos en listas negras y blancas.

4.5.4. Entregables

Durante la vigencia del contrato la contratista deberá proporcionar al Administrador del Contrato los siguientes documentos:

Entregable	Plazo
Informe técnico de Renovación de las licencias de la Suite de Seguridad ESET Endpoint Protection Advanced y el certificado	máximo en 3 días calendario posteriores a la firma del contrato
Informes de trabajo por cada soporte técnico solicitado	Máximo 1 día calendario posteriores a la realización del soporte técnico.
Acta de Transferencia de Conocimientos, certificados de participación	8 días calendario posterior a la transferencia de conocimientos

CORPORACIÓN FINANCIERA NACIONAL

Cláusula Quinta.- PRECIO DEL CONTRATO

5.1. El valor del presente contrato, que la CONTRATANTE pagará al CONTRATISTA, es el de **USD$ 45,927.04 (Cuarenta y Cinco Mil Novecientos Veintisiete 04/100 DÓLARES DE LOS ESTADOS UNIDOS DE AMERICA)** más IVA, de conformidad con la oferta presentada por la CONTRATISTA:

ÍTEM	DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO SIN IVA
1	ESET ENDPOINT PROTECTION ADVANCED	1128	$ 9.7	$ 10,941.60
2	DESLOCK PRO	358	$ 27.00	$ 9,666.00
3	DESLOCK STANDARD	590	$ 15.00	$ 8,850.00
4	ESET ENTERPRISE INSPECTOR	1128	$ 13.98	$ 15,769.44
5	ACTUALIZACION Y CONFIGURACION	1	$ 700.00	$ 700.00
			SUBTOTAL	$ 45,927.04
			IVA 12%	$ 5,511.24
			TOTAL	$ 51,438.28

5.2. Los precios acordados en el contrato, constituirán la única compensación a la CONTRATISTA por todos sus costos, inclusive cualquier impuesto, derecho o tasa que tuviese que pagar, excepto el Impuesto al Valor Agregado que será añadido al precio del contrato.

Cláusula Sexta.- FORMA DE PAGO:

6.1. Los valores que la CFN B.P. cancele al contratista por efecto de las obligaciones contratadas se realizarán conforme se detalla a continuación:

- El 60% del total de la contratación, una vez presentado por la contratista el Informe Técnico junto con el certificado de renovación, en el que certifique la renovación y entrega del licenciamiento, acta entrega recepción suscrita entre la contratista y el administrador, informe de conformidad del administrador del contrato y la presentación de la factura correspondiente.

- El 30% del total de la contratación, una vez presentado por la contratista el Informe Técnico en el que certifique la instalación y configuración de las licencias, acta entrega recepción suscrita entre el contratista y el administrador, informe de conformidad del administrador del contrato y la presentación de la factura correspondiente.

- El 10% se pagará a la finalización del contrato, previa presentación del informe a conformidad del administrador del contrato, acta de entrega recepción definitiva y la factura correspondiente.

Para el pago final, deberá adjuntarse, la respectiva acta de entrega recepción definitiva del contrato, misma que deberá ser elaborada por el Administrador del contrato y suscrita de acuerdo a lo establecido en el artículo 124 del Reglamento General de la Ley del Sistema Nacional de Contratación Pública.

De los pagos que se deba hacer, la contratante retendrá las multas que procedan de acuerdo con el contrato, así como las retenciones de ley que correspondan.

Todos los pagos que se hagan a la contratista por cuenta del contrato, se efectuarán con sujeción al precio convenido, a

satisfacción de la contratante, previa aprobación del administrador del contrato.

Pagos indebidos: El CONTRATANTE se reserva el derecho de reclamar al CONTRATISTA, en cualquier tiempo, antes o después de la prestación del servicio, sobre cualquier pago indebido por error de cálculo o por cualquier otra razón, debidamente justificada, obligándose la contratista a satisfacer las reclamaciones que por este motivo llegare a plantear EL CONTRATANTE, reconociéndose el interés calculado a la tasa máxima del interés convencional, establecido por el Banco Central del Ecuador.

La Corporación Financiera Nacional B.P. realizará las retenciones respectivas de acuerdo a las normativas aplicables especificadas en la Ley de Régimen Tributario Interno.

Cláusula Séptima. - GARANTÍAS

Las garantías que la Contratista debe presentar son:

7.1. Garantía Técnica

La contratista deberá entregar al administrador del contrato, dentro de los primeros 3 días hábiles posterior a la firma del contrato, la Garantía Técnica (Ver Anexo 6 de los pliegos) del servicio por el tiempo que dure el contrato; garantía que avale el buen funcionamiento y disponibilidad del servicio; en base a los términos detallados en el presente documento y términos de referencia, junto con el informe y certificado de renovación de las licencias.

Para la garantía técnica, la CFN B.P. no asumirá costo adicional para las actualizaciones de software, firmware, parches de seguridad o mano de obra; estos costos deben ser asumidos por el proveedor adjudicado.

7.1.1. Ejecución de las garantías: Las garantías contractuales podrán ser ejecutadas por la contratante en los siguientes casos:

7.1.2. La Técnica:

a) Cuando se incumpla con el objeto de esta garantía, de acuerdo con lo establecido en el pliego y este contrato.

7.2. Las garantías entregadas se devolverán de acuerdo a lo establecido en el artículo 77 de la Ley Orgánica del Sistema Nacional de Contratación Pública y 118 del Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Pública. Entre tanto, deberán mantenerse vigentes, lo que será vigilado y exigido por la contratante.

Cláusula Octava.- PLAZO

8.1. El plazo para la ejecución del presente contrato es de 733 días contados a partir de la suscripción de su suscripción, el cual se ejecutará de la siguiente manera:

- Dentro del plazo máximo de tres (3) días calendarios contados a partir de la suscripción del contrato, la Contratista deberá entregar el certificado de renovación, en el que certifique la renovación y entrega del licenciamiento de la Suite de Seguridad ESET Endpoint Protection Advanced con las que cuenta la institución.
- El plazo de setecientos treinta (730) días calendario, para la vigencia del licenciamiento de la Suite de Seguridad ESET Endpoint Protection Advanced, que serán contados a partir de la fecha de entrega del certificado de renovación y entrega de las licencias, lo que se indicará en el informe técnico del contratista. Cabe indicar que durante la vigencia del licenciamiento y posterior a la entrega del certificado de renovación, la contratista dispondrá un plazo no mayor a veinte (20) días, para realizar la instalación y configuración de las licencias en los equipos de usuario final

Cláusula Novena. - PRÓRROGAS DE PLAZO

9.1. La contratante prorrogará el plazo total o los plazos parciales en los siguientes casos:

a) Cuando la contratista así lo solicitare, por escrito, justificando los fundamentos de la solicitud, dentro del plazo de quince días siguientes a la fecha de producido el hecho, siempre que este se haya producido por motivos de fuerza mayor o caso fortuito aceptado como tal por la máxima autoridad de la entidad contratante o su delegado, previo informe del administrador del contrato. Tan pronto desaparezca la causa de fuerza mayor o caso fortuito, el contratista está obligado a continuar con la ejecución del contrato, sin necesidad de que medie notificación por parte del administrador del contrato para reanudarlo.

b) Por suspensiones en la ejecución del contrato, motivadas por la contratante u ordenadas por ella y que no se deban a causas imputables al contratista.

c) Si la contratante no hubiera solucionado los problemas administrativos-contractuales en forma oportuna, cuando tales circunstancias incidan en la ejecución del trabajo.

9.2. En casos de prórroga de plazo, las partes elaborarán un nuevo cronograma, de ser el caso, que suscrito por ellas, sustituirá al original o precedente y tendrá el mismo valor contractual del sustituido. Y en tal caso se requerirá la autorización de la máxima autoridad de la contratante, previo informe del administrador del contrato.

Cláusula Décima.- MULTAS

10.1. Las multas deberán aplicarse de la siguiente forma:

Por falta de cumplimiento de los servicios, entregables, cronograma; la contratista cancelará una multa del 1x1000 por cada día de retraso, sobre el porcentaje de las obligaciones que se encuentren pendientes de ejecutarse conforme a lo establecido en el contrato, excepto en el evento de caso fortuito o fuerza mayor, conforme lo dispuesto en el artículo 30 de la Codificación del Código Civil, debidamente comprobado y aceptado por el CONTRATANTE, para lo cual se notificará dentro quince (15) días subsiguientes de ocurridos los hechos. Una vez transcurrido este plazo, de no mediar dicha notificación, se entenderá como no ocurridos los hechos que alegue la CONTRATISTA como causa para la no ejecución de la provisión del servicio y se le impondrá la multa prevista anteriormente.

En caso de existir indisponibilidad del servicio, incumplimiento en los tiempos de atención o resolución de incidentes, definidos en el Acuerdo de Nivel de Servicios SLA, la contratante descontará los valores, que serán descontados de los pagos correspondientes.

Si el valor de las multas impuestas llegare a superar el valor equivalente al 5% del monto total del contrato, la CFN B.P. podrá dar por terminado este contrato de manera anticipada y unilateral, y declarar incumplido al contratista.

La contratista autoriza expresamente a la CFN B.P. para que descuente el valor correspondiente a las multas de la o las planillas que se presenten para el pago cuando apliquen.

Cláusula Décima Primera.- DEL REAJUSTE DE PRECIOS.

11.1. Para efectos del presente contrato y por su forma de pago, no habrá reajuste de precios.

Cláusula Décima Segunda.- SUBCONTRATACIÓN

12.1. La CONTRATISTA podrá subcontratar determinados trabajos previa autorización de la entidad contratante siempre que el monto de la totalidad de lo subcontratado no exceda del 30% del valor total del contrato principal, y el subcontratista esté habilitado en el RUP.

12.2. La CONTRATISTA será el único responsable ante el CONTRATANTE por los actos u omisiones de sus subcontratistas y de las personas directa o indirectamente empleadas por ellos.

Cláusula Décima Tercera.- DE LA ADMINISTRACIÓN DEL CONTRATO

13.1. La CONTRATANTE designará al administrador del contrato, quien deberá atenerse a las Condiciones Generales y Particulares del pliego que forman parte del presente contrato, y velará por el cabal cumplimiento del mismo en base a lo dispuesto en el artículo 121 de Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Pública.

13.2 La CONTRATANTE podrá cambiar de administrador del contrato, para lo cual bastará notificar a la CONTRATISTA la respectiva comunicación; sin que sea necesario la modificación del texto contractual.

Cláusula Décima Cuarta.- OTRAS OBLIGACIONES DE LA CONTRATISTA

En virtud de la celebración del contrato, la contratista se obliga:

14.1 La contratista se compromete a ejecutar el contrato derivado del procedimiento de contratación tramitado, sobre la base de los términos de referencia elaborados por la entidad contratante y que fueron conocidos en la etapa precontractual; y en tal virtud, no podrá aducir error, falencia o cualquier inconformidad con los mismos, como causal para solicitar ampliación del plazo, o contratos complementarios. La ampliación del plazo, o contratos complementarios podrán tramitarse solo si fueren aprobados por el administrador del contrato.

14.2. La contratista se compromete durante la ejecución del contrato, a facilitar a las personas designadas por la entidad contratante, toda la información y documentación que éstas soliciten para disponer de un pleno conocimiento técnico relacionado con la ejecución del contrato, así como de los eventuales problemas técnicos que puedan plantearse y de las tecnologías, métodos y herramientas utilizadas para resolverlos.

Los delegados o responsables técnicos de la entidad contratante, como el administrador del contrato, deberán tener el conocimiento suficiente de la ejecución del contrato, así como la eventual realización de ulteriores desarrollos. Para el efecto, el contratista se compromete durante el tiempo de ejecución contractual, a facilitar a las personas designadas por la entidad contratante toda la información y documentación que le sea requerida, relacionada y/o atinente al desarrollo y ejecución del contrato.

14.3. Queda expresamente establecido que constituye obligación del contratista ejecutar el contrato conforme a las especificaciones técnicas o términos de referencia establecidos en el pliego, y cumplir con el porcentaje mínimo de Valor Agregado Ecuatoriano ofertado, de ser el caso.

14.4. La contratista está obligada a cumplir con cualquiera otra que se derive natural y legalmente del objeto del contrato y sea exigible por constar en cualquier documento del mismo o en norma legal específicamente aplicable.

14.5 La Contratista se obliga al cumplimiento de las disposiciones establecidas en el Código del Trabajo y en la Ley de Seguridad Social obligatorio, adquiriendo, respecto de sus trabajadores, la calidad de patrono, sin que la contratante tenga responsabilidad alguna por tales cargas, ni relación con el personal que labore en la ejecución del contrato, ni con el personal de la subcontratista.

14.6. La contratista se obliga al cumplimiento de lo exigido en el pliego, a lo previsto en su oferta y a lo establecido en la legislación ambiental, de seguridad industrial y salud ocupacional, seguridad social, laboral, etc.

14.7. La Contratista se obliga además con la Contratante a cumplir lo establecido en los respectivos Acuerdos de Niveles de Servicio; Transferencia de Conocimientos, Confidencialidad de la Información y datos; y, Derechos de propiedad intelectual del conocimiento, productos, datos e información.

Cláusula Décima Quinta.- OBLIGACIONES DE LA CONTRATANTE

En virtud de la celebración del contrato, la contrante se obliga:

15.1. Brindar las facilidades y accesos correspondientes para que el personal técnico del proveedor realice las actividades de actualización configuración y transferencia de conocimientos.

15.2. La entidad contratante dispone de 5 días calendarios, luego de la firma del contrato, para proporcionar los documentos, accesos e información como por ejemplo número de equipos, ubicación, nombres y direcciones ip de los mismos, que el contratista requiera.

CORPORACIÓN FINANCIERA NACIONAL

Cláusula Décima Sexta.- CONTRATOS COMPLEMENTARIOS

16.1. Por causas justificadas, las partes podrán firmar contratos complementarios de conformidad con lo establecido en los artículos 85 y 87, de la LOSNCP, y en los artículos 144 del RGLOSNCP; y todas las Resoluciones y Actualizaciones que se encuentren vigentes aplicables a la mencionada Ley (*Ley Orgánica para la Eficiencia en la Contratación Pública*, Registro Oficial N° 966 del 20 de marzo del 2017).

Cláusula Décima Séptimo.- RECEPCIÓN DEFINITIVA DEL CONTRATO

17.1 Para el pago final se deberá suscribir la respectiva Acta de entrega Recepción Definitiva del Contrato, suscrita por el contratista y los integrantes de la comisión designada por la contratante, en los términos del artículo 124 del Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Pública.

17.2 LIQUIDACIÓN DEL CONTRATO: La liquidación final del contrato suscrita entre las partes se realizará en los términos previstos por el artículo 125 del Reglamento General de la Ley Orgánica del Sistema Nacional de Contratación Pública.

Cláusula Décima Octava.- TERMINACIÓN DEL CONTRATO

18.1. Terminación del contrato.- El contrato termina conforme lo previsto en el artículo 92 de la Ley Orgánica del Sistema Nacional de Contratación Pública y las Condiciones Particulares y Generales del Contrato.

18.2. Causales de Terminación unilateral del contrato.-Tratándose de incumplimiento de la CONTRATISTA, procederá la declaración anticipada y unilateral del CONTRATANTE, en los casos establecidos en el artículo 94 de la LOSNCP. Además, se considerarán las siguientes causales:

a) Si la CONTRATISTA no notificare al CONTRATANTE acerca de la transferencia, cesión, enajenación de sus acciones, participaciones, o en general de cualquier cambio en su estructura de propiedad, dentro de los cinco días hábiles siguientes a la fecha en que se produjo tal modificación;

b) Si el CONTRATANTE, en función de aplicar lo establecido en el artículo 78 de la LOSNCP, no autoriza la transferencia, cesión, capitalización, fusión, absorción, transformación o cualquier forma de tradición de las acciones, participaciones o cualquier otra forma de expresión de la asociación, que represente el veinticinco por ciento (25%) o más del capital social de la CONTRATISTA;

c) Si se verifica, por cualquier modo, que la participación ecuatoriana real en la ejecución de la obra objeto del contrato es inferior a la declarada o que no se cumple con el compromiso de subcontratación asumido en el formulario de oferta, y en esa medida se ha determinado que la CONTRATISTA no cumple con la oferta;

d) Si la CONTRATISTA incumple con las declaraciones que ha realizado en el numeral 1.1 del Formulario de Oferta - Presentación y Compromiso; y,

e) El caso de que la entidad contratante encontrare que existe inconsistencia, simulación y/o inexactitud en la información presentada por la contratista, en el procedimiento precontractual o en la ejecución del presente contrato, dicha inconsistencia, simulación y/o inexactitud serán causales de terminación unilateral del contrato por lo que, la máxima autoridad de la entidad contratante o su delegado, lo declarará contratista incumplido, sin perjuicio además, de las acciones judiciales a que hubiera lugar.

18.3. Procedimiento de terminación unilateral.-El procedimiento a seguirse para la terminación unilateral del contrato será el previsto en el artículo 95 de la LOSNCP.

18.4. La declaratoria de terminación unilateral y anticipada del contrato no se suspenderá por la interposición de reclamos o recursos administrativos, demandas contencioso administrativas, arbitrales o de cualquier tipo de parte de la contratista.

18.5. Tampoco se admitirá acciones constitucionales contra las resoluciones de terminación unilateral del contrato, porque se tienen mecanismos de defensas adecuados y eficaces para proteger los derechos derivados de tales resoluciones, previstos en la Ley.

18.6. Terminación por Mutuo Acuerdo del Contrato.- Cuando por circunstancias imprevistas, técnicas o económicas, o causas de fuerza mayor o caso fortuito, no fuere posible o conveniente para los intereses de las partes, ejecutar total o parcialmente, el contrato, las partes podrán, por mutuo acuerdo, convenir en la extinción de todas o algunas de las obligaciones contractuales, de conformidad con lo establecido en el artículo 93 de la Ley Orgánica del Sistema Nacional de Contratación Pública.

Cláusula Decima Novena. - SOLUCIÓN DE CONTROVERSIAS

19.1. De suscitarse cualquier divergencia o controversia que no se haya podido solucionar a través de la participación activa y directa de las partes, estas podrán utilizar los métodos alternativos para la solución de controversias, pudiendo someterse a la mediación a través del Centro de Mediación de la Procuraduría General del Estado; siendo aplicables las disposiciones de la Ley de Arbitraje y Mediación, y del Reglamento del indicado Centro de Mediación.

19.2. Si respecto de la divergencia o controversia existente no se lograre un acuerdo directo entre las partes, éstas se someterán al procedimiento contencioso administrativo contemplado en el Código Orgánico General de Procesos; o la normativa que corresponda; siendo competente para conocer la controversia el Tribunal Distrital de lo Contencioso Administrativo que ejerce jurisdicción en el domicilio de la Entidad del sector público.

19.3 La legislación aplicable a este contrato es la ecuatoriana. En consecuencia, el contratista declara conocer el ordenamiento jurídico ecuatoriano y por lo tanto, se entiende incorporado el mismo en todo lo que sea aplicable al presente contrato.

Cláusula Vigésima.- COMUNICACIONES ENTRE LAS PARTES

20.1. Todas las comunicaciones, sin excepción, entre las partes, relativas a los trabajos realizados, serán formuladas por escrito o por medios electrónicos y en idioma español. Las comunicaciones entre el administrador del contrato y el contratista se harán a través de documentos escritos, o por medios electrónicos.

Cláusula Vigésima Primera.-TRIBUTOS, RETENCIONES Y GASTOS

21.1. El CONTRATANTE efectuará a la CONTRATISTA las retenciones que dispongan las leyes tributarias, actuará como agente de retención del Impuesto a la Renta e Impuesto al Valor Agregado, al efecto procederá conforme la legislación tributaria vigente.

El CONTRATANTE retendrá el valor de los descuentos que el Instituto Ecuatoriano de Seguridad Social ordenare y que corresponda a mora patronal, por obligaciones con el seguro social provenientes de servicios personales para la ejecución del contrato de acuerdo a la Ley de Seguridad Social.

21.2. Es de cuenta de la CONTRATISTA el pago de los gastos notariales, de las copias certificadas del contrato y los documentos que deban ser protocolizados, en caso de ser necesario. La CONTRATISTA entregará al CONTRATANTE hasta cinco copias de este contrato, debidamente protocolizadas. En caso de terminación por mutuo acuerdo, el pago de los derechos notariales y el de las copias será de cuenta de la CONTRATISTA.

Cláusula Vigésima Segunda.- DOMICILIO

22.1. Para todos los efectos de este contrato, las partes convienen en señalar su domicilio en la ciudad de Guayaquil.

22.2. Asimismo, para efectos de comunicación o notificaciones, las partes señalan como su dirección, las siguientes:

EL CONTRATANTE: Avenida 9 de octubre No. 200 entre Pichincha y Pedro Carbo Edificio Corporación Financiera Nacional B.P. Teléfono: 042560888.

LA CONTRATISTA: Jerónimo Carrión, E8-132, Av. 6 de Diciembre / Teléfono: 022227766 / Correo electrónico: info@inforc.ec

Las comunicaciones también podrán efectuarse a través de medios electrónicos, específicamente a través del email del Administrador del Contrato. La dirección electrónica será comunicada en forma inmediata a la Contratista por el Administrador del Contrato tan pronto sea designado. Si en el contrato ya está establecido quién es el Administrador, deberá hacer conocer de forma inmediata su dirección electrónica a la CONTRATISTA, ésta a su vez deberá notificar al Administrador su dirección electrónica en forma inmediata a la recepción de la dirección electrónica.

22.3. La CONTRATISTA, se obliga en forma incondicional a la CONTRATANTE, el cambio de dirección para efectos de comunicaciones y notificaciones, en relación con la dirección que consta descrita en el contrato. Si la Contratista no notificare dicho al CONTRATANTE cambio, se entiende para todos los efectos constitucionales, legales y contractuales que todas las notificaciones que la le haga a la CONTRATANTE a la CONTRATISTA en la dirección que consta en el Contrato son plenamente válidas y eficaces jurídicamente.

La CONTRATISTA deja constancia que no podrá alegar válidamente el desconocimiento del contenido de las notificaciones y sus anexos que le haga la CONTRATANTE en la dirección descrita en el contrato, no pudiendo, por ello, la CONTRATISTA alegar nulidad del procedimiento respectivo.

Cláusula Vigésima Tercera.- ACEPTACIÓN DE LAS PARTES

23.1. Declaración.- Las partes libre, voluntaria y expresamente declaran que conocen y aceptan el texto íntegro de las condiciones del presente contrato, así como de los documentos que forman parte integrante del mismo.

23.2. Libre y voluntariamente, las partes expresamente declaran su aceptación a todo lo convenido en el presente contrato y se someten a sus estipulaciones.

Dado, en la ciudad de Guayaquil, a los 14 días de mes de febrero del 2020

Por la Contratante
CORPORACIÓN FINANCIERA NACIONAL
B.P.
RUC: 1760003090001

Ing. Grace Ivonne Rodríguez Barcos
Delegada del Gerente General

Por el Contratista
ITSEGUINFO CIA. LTDA.
RUC: 1790935426001

Carlos Jumbo Guaycha
Representante Legal