CORPORACIÓN FINANCIERA NACIONAL

INFORME DE CONVENIENCIA Y VIABILIDAD TÉCNICA-ECONÓMICA PARA LA CONTRATACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL.

A fin de cumplir con la Regulación DIR-014-2019 de fecha 06 de marzo de 2019, respecto del REGLAMENTO INTERNO DE CONTRATACIONES POR GIRO ESPECÍFICO DE NEGOCIO publicado en Registro Oficial el 29 de marzo de 2019 mediante Edición Especial 841, en su Título III DE LOS PROCEDIMIENTOS DE CONTRATACIÓN, Capítulo XI DE LAS CONTRATACIONES INTERADMINISTRATIVAS, en el Artículo 105, numeral 2, establece:

"La Corporación Financiera Nacional B.P., podrá en el ámbito de aplicación del presente Reglamento Interno y de acuerdo al procedimiento previsto en el capítulo, contratar de manera directa, la ejecución de obras, adquisición de bienes o prestación de servicios, incluidos los de consultoría con: 2. Empresas públicas o las empresas cuyo capital suscrito pertenezca, por lo menos en cincuenta por ciento (50%) a entidades de derecho público;

Dentro del ámbito de competencia de la Gerencia de Tecnologías de la Información, se presenta el informe de conveniencia y viabilidad técnica-económica para la contratación del **SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL.**

1. ANTECEDENTES Y JUSTIFICACIÓN

La Corporación Financiera Nacional B.P., es una institución financiera pública, cuya misión consiste en impulsar el desarrollo de los sectores productivos y estratégicos del Ecuador, a través de múltiples servicios financieros y no financieros alineados a las políticas públicas. Para poder cumplir con sus objetivos institucionales, usa diferentes servicios y herramientas tecnológicas para de esta manera servir a sus clientes de manera eficiente ágil y oportuna.

La dependencia de la Corporación Financiera Nacional B.P (CFN B.P.) respecto de los sistemas y servicios de información, obliga a tomar medidas que permitan garantizar la disponibilidad de los servicios mediante infraestructura tecnológica de hardware y software que cumpla con:

- Políticas de Tecnología de Información
- Políticas de Seguridad de la Información
- Plan Estratégico de Tecnología Informática – PETI
- Plan Estratégico de Seguridad de la Información
- Normativa Interna para la Seguridad de la Información
- Resolución de la Superintendencia de Bancos, sobre la gestión del riesgo operativo en las instituciones financieras y públicas, dentro de la cual se considera como un factor de riesgo operativo a la tecnología de información
- Normativa de la Contraloría General del Estado

La Corporación Financiera Nacional B.P. basa su organización en un esquema de gestión por procesos; en tal sentido, la contratación del Servicio de Seguridad

Perimetral Gerenciada está apalancada en el macroproceso de Gestión de Tecnología de la Información y sus subprocesos de Operar servicios de TI y Gestionar servicios de seguridad. Adicionalmente, los principales activos de la Institución que se están protegiendo con estos servicios de seguridad son:

- Red de datos institucional a nivel nacional
- Red institucional extendida desde sitios remotos
- Servicios del aplicativo core bancario a nivel nacional
- Servicio de navegación a nivel nacional
- Aplicaciones web institucionales
- Mensajería interna vía correo electrónico

La contratación del Servicio de Seguridad Perimetral Gerenciada permitirá a la institución asegurar el adecuado cumplimiento de los parámetros de seguridad de la información en cuanto a:

- **Disponibilidad:** permitiendo que los servicios de tecnologías de la información se mantengan operando sin sufrir ninguna degradación en cuanto a accesos. Así también se permitirá habilitar los recursos que requieran los usuarios autorizados cuando así lo requieran. De esta manera se previenen posibles interrupciones no autorizadas de los recursos informáticos.
- **Integridad:** asegurando que la información se mantenga inalterada ante accidentes o intentos maliciosos de acceso. De esta manera se previenen posibles modificaciones no autorizadas de la información.
- **Confidencialidad:** certificando que la información sea accesible de únicamente a las personas que se encuentran autorizadas. De esta manera, se previene la divulgación no autorizada de la información de nuestra institución.

Se presentan a continuación los principales riesgos de no poder contar con el Servicio de Seguridad Perimetral Gerenciada:

- No contar con el servicio de cortafuegos, hace que la CFN se muestra vulnerable a ataques hacia su infraestructura tecnológica institucional comprometiendo la disponibilidad y la confidencialidad de la información.
- No contar con un adecuado filtrado de contenido y control de aplicaciones podría facilitar accesos no autorizado a información de la institución, comprometiendo su confidencialidad. Adicionalmente, un inadecuado control del ancho de banda generaría retardo en los aplicativos y servicios expuestos de la red, comprometiendo su disponibilidad.
- Controles deficientes tanto de mensajes no deseados y como de malware podría provocar divulgación no autorizada de la información de nuestra institución, comprometiendo su confidencialidad. Adicionalmente, no contar con el servicio de antivirus/antispam perimetral podría causar la indisponibilidad del servicio de correo electrónico institucional, comprometiendo su disponibilidad.

- No asegurar la adecuada conectividad de los usuarios internos y externos a la red institucional podría provocar intentos maliciosos de acceso, comprometiendo la integridad de la información.
- La carencia de un sistema para la prevención de intrusiones en la red institucional o los servicios informáticos dejaría a la institución vulnerable ante posibles ataques informáticos comprometiendo la disponibilidad y confidencialidad de la información.
- No contar con un servicio que aísle, controle y mitigue posibles ataques en un ambiente controlado permitiría el acceso no autorizado a información de la institución, comprometiendo su confidencialidad. Adicionalmente, la denegación del servicio podría provocar retardo en los aplicativos web de la institución, comprometiendo su disponibilidad.
- El no disponer de una solución que permita controlar en la periferia las peticiones de Internet hacia las aplicaciones web institucionales podría provocar inconvenientes de denegación del servicio, comprometiendo la disponibilidad e integridad de la información.
- No contar con datos e información oportuna para toma de decisiones y notificación a organismos de control podría generar incumplimientos normativos que acarrearían observaciones a la Institución.

2. BASE LEGAL

El numeral 6 de la sección 410-09: "Mantenimiento y control de la infraestructura tecnológica", subgrupo 410: "TECNOLOGÍA DE LA INFORMACIÓN", grupo 400: "ACTIVIDADES DE CONTROL" de las "Normas de Control Interno para las Entidades, Organismos del Sector Público", de la Contraloría General del Estado, establece textualmente que: "*Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad*", considerando que la unidad de tecnología de información de cada organización será la responsable de definir y regular los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades.

En el "LIBRO I: NORMATIVA SOBRE OPERACIONES, TITULO IV: ADMINISTRACIÓN DE RIESGOS, SUBTITULO V: SEGURIDAD DE INFORMACIÓN (DIR-032-2010), CAPÍTULO I: MANUAL DE SEGURIDAD DE LA INFORMACIÓN, SECCIÓN I: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN", de la Normativa de la CFN B.P., Numeral "5. DE LA SEGURIDAD FÍSICA Y DEL ENTORNO, D. POLITICAS GENERALES", Sección "Seguridad del equipamiento y documentación", establece textualmente que: "*d) El equipamiento será provisto de mantenimiento adecuado para asegurar que su disponibilidad e integridad sean permanentes.*"

Por otro lado, 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, CAPÍTULO V.- NORMA DE CONTROL PARA LA GESTION DEL RIESGO OPERATIVO, la Superintendencia de Bancos, establece textualmente:

"SECCION *III.- FACTORES DEL RIESGO OPERATIVO*
ARTICULO 10, literal c. Tecnología de la Información Las entidades controladas deben contar con tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros esté disponible para la toma de decisiones.

(...) iii. Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de las entidades controladas, se debe implementar al menos lo siguiente: Procedimientos que establezcan las actividades y responsable de la operación y el uso de los centros de datos, que incluyan controles que eviten accesos no autorizados;

(...) v. Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las entidades controladas deben implementar al menos: Infraestructura que soporta los procesos críticos con la redundancia necesaria para evitar puntos únicos de falla; de la cual se debe mantener el inventario y respaldos de la configuración actualizada e informes de su mantenimiento periódico; en el caso de los enlaces de comunicación, debe considerar que la trayectoria de los enlaces principal y alterno sean diferentes; procedimientos que permitan la administración y monitoreo de las bases de datos, redes de datos, hardware y software base, que incluya límites y alerta."

SECCIÓN VII.- SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 16.- Las entidades controladas deben establecer, implementar, operar, monitorear, mantener y mejorar un sistema de gestión de seguridad de la información que incluya al menos lo siguiente:

(...) ***j.*** *Para considerar la existencia de un apropiado ambiente de gestión de seguridad de la información, la unidad responsable de la seguridad de la información debe implementar:*

> ***vi.*** *Procedimientos para el uso, protección y tiempo de vida de las llaves criptográficas utilizadas para cifrar la información;*
>
> ***vii.*** *Técnicas de cifrado sobre la información que lo requiera como resultado del análisis de riesgos de seguridad;*
>
> ***x.*** *Con base en un análisis de riesgos, realizar la segmentación de la red de datos y la implementación de sistemas de control y autenticación tales como: sistemas de prevención de intrusos (IPS), firewalls, firewall de*

aplicaciones web (WAF), entre otros; para evitar accesos no autorizados inclusive de terceros y ataques externos especialmente a la información crítica;

xiii. *Procedimientos de gestión de incidentes de seguridad de la información, en los que se considere al menos: reporte de eventos, su evaluación, registro de incidentes, comunicación, priorización, análisis, respuesta y recolección de evidencias.,*

SECCIÓN VIII.- SEGURIDAD EN CANALES ELECTRÓNICOS

ARTÍCULO 17.- Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles y mecanismos para evitar el cometimiento de eventos fraudulentos o no autorizados por los usuarios y garantizar la seguridad de la información, así como los bienes de los clientes a cargo de las entidades controladas, éstas deben cumplir como mínimo con lo siguiente: (Reformado por Resolución No. SB-2019-497, de 29 de abril de 2019)

a. *Las entidades controladas deben adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento;*
b. *Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad; se debe generar informes trimestrales dirigidos al comité de seguridad;*
c. *Canales de comunicación seguros mediante la utilización de técnicas de cifrado acorde con los estándares internacionales vigentes;*
e. *El envío de información de sus clientes relacionada con al menos números de cuentas y tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía internet, ésta deberá ser enmascarada;*
f. *La información confidencial que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de cifrado acordes con los estándares internacionales vigentes y deberá evaluarse con regularidad la efectividad del mecanismo utilizado;*
g. *Las entidades controladas deben contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la entidad;*
h. *Las entidades controladas deben utilizar tecnología de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información en todo momento debe estar cifrada;*

i. *Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas;*
u. *Las entidades controladas deben enviar a sus clientes mensajes en línea a través de mensajería móvil, correo electrónico u otro mecanismo, notificando la ejecución de transacciones monetarias realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas;*

El Esquema Gubernamental de Seguridad de la Información EGSI en su numeral 2.3 sobre las responsabilidades del responsable de Seguridad del Área de Tecnologías de la Información indica lo siguiente:
h) Implementar los controles de seguridad definidos (ej., evitar software malicioso, accesos no autorizados, etc.)
j) Gestionar los incidentes de seguridad de la información de acuerdo a los procedimientos establecidos.

En base a lo expuesto, la Corporación Financiera Nacional B.P. mantiene sus servicios operativos protegidos por medio del Servicio de Seguridad Perimetral Gerenciada, debido a la importancia de la información institucional es necesario mantener un control sobre toda la red y brindar confidencialidad, disponibilidad, integridad para el control de acceso a usuarios permitidos, transacciones con enlaces interinstitucionales, acceso web a sitios conocidos y categorizados como confiables, minimizando el riesgo de infiltraciones en la red.

Con la finalidad de garantizar la seguridad, disponibilidad y rendimiento de los servicios que la CFN B.P. provee, el servicio de Seguridad Perimetral es considerado como crítico; así también, es necesario dar cumplimiento a las recomendaciones de los organismos de control; por lo tanto, se pone en evidencia la necesidad de iniciar el proceso de contratación del SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL

3. CARACTERÍSTICAS TÉCNICAS DEL SERVICIO REQUERIDO

CFN B.P. requiere de un esquema de seguridad que considere tanto los mecanismos activos de protección, así como de componentes de control y administración para asegurar su plataforma de comunicación e información; por lo tanto, el Servicio de Seguridad Perimetral Gerenciada a nivel nacional deberá incluir:

Los **mecanismos activos** de protección que CFN B.P. requiere son los siguientes:

- Cortafuegos (Firewall) de siguiente generación en un esquema de Alta Disponibilidad (HA) en modo Activo /Pasivo, tanto en Quito como en Guayaquil.
- Balanceo de carga de enlaces para tráfico saliente
- Acceso VPN IPSEC, VPN SSL
- Filtrado de navegación Web con inspección de contenido SSL
- Control de Aplicación con mecanismos y firmas para Anti-Bot
- Protección contra Intrusos (IPS)
- Antivirus Perimetral
- Antivirus y Antispam para correo electrónico

- Web Application Firewall con protección de contra ataques distribuidos de denegación de servicio (DDOS) a nivel de aplicación.

Los **componentes de control y administración** que CFN B.P. requiere son los siguientes:

- Sistema de analítica y manejo avanzado de reportes, que mediante correlación de registros de seguridad (Security Logs) facilite la gestión y evidencia los incidentes de seguridad que se presentan en el perímetro de la red de la CFN B.P.
- Sistema de emulación de incidentes de seguridad (Sandboxing), que permita revisar y reproducir en un ambiente seguro las variables de un ataque con el objetivo de robustecer la plataforma contra las mismas.

El resumen de servicios a recibir son los siguientes:

#	Servicio de Seguridad Perimetral Gerenciada	Cantidad (meses)
1	Cortafuegos (Firewall) de siguiente generación en un esquema de Alta Disponibilidad (HA) en modo Activo /Pasivo, tanto en Quito como en Guayaquil	24
2	Balanceo de carga de enlaces para tráfico saliente	24
3	Acceso VPN IPSEC	24
4	VPN SSL	24
5	Filtrado de navegación Web con inspección de contenido SSL	24
6	Control de Aplicación con mecanismos y firmas para Anti-Bot	24
7	Protección contra Intrusos (IPS)	24
8	Antivirus Perimetral	24
9	Antivirus y Antispam para correo electrónico	24
10	Web Application Firewall con protección de contra ataques distribuidos de denegación de servicio (DDOS) a nivel de aplicación	24
12	Sistema de analítica y manejo avanzado de reportes	24
13	Sistema de emulación de incidentes de seguridad (Sandboxing)	24
14	Licenciamiento	24
15	Monitoreo Proactivo	24
16	Security Operation Center (SOC)	24
17	Administración Compartida	24
19	Mantenimiento Preventivo (1 vez al año)	2
20	Mantenimiento Correctivo (24x7)	24
21	Transferencia de conocimientos	1

A continuación, los diagramas de arquitectura de la solución:

Diagrama 1: Arquitectura de Seguridad Gerenciada - CFN B.P. Quito

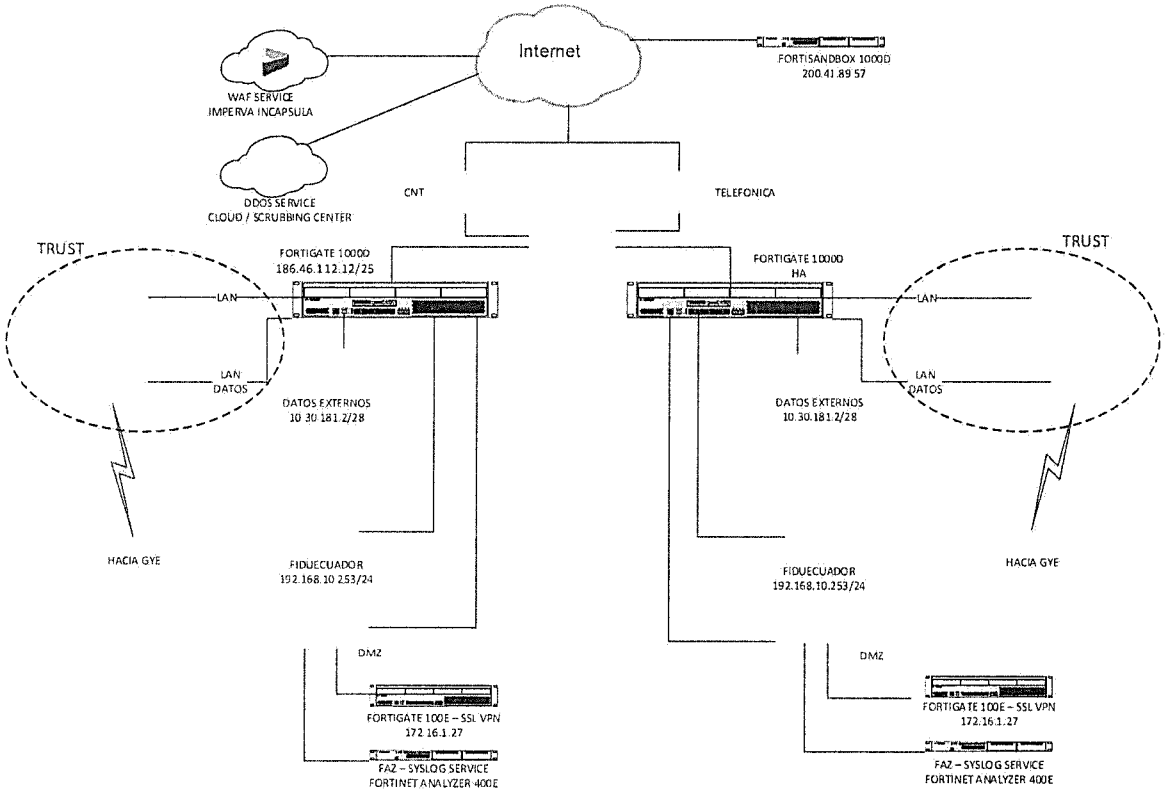
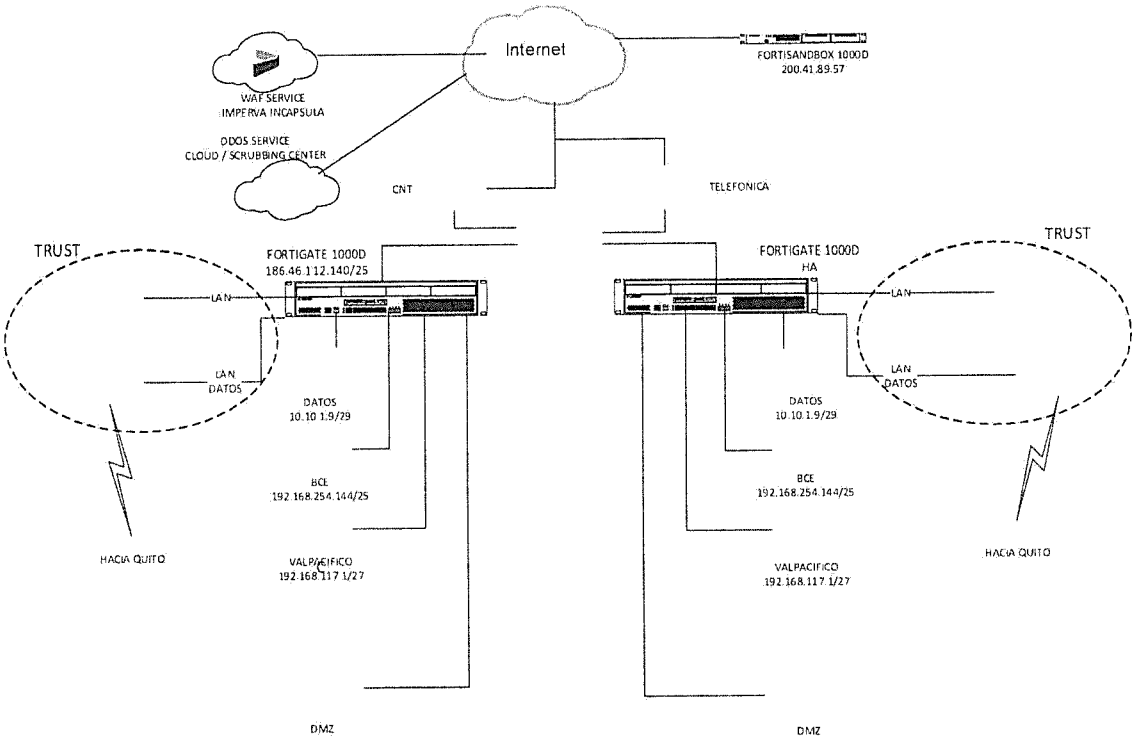


Diagrama 2: Arquitectura de Seguridad Gerenciada – CFN B.P. Guayaquil



4. COTIZACIONES RECIBIDAS

Mediante correo electrónico, el 23 de enero de 2020, se recibió la cotización del proveedor CNT E.P., por un valor de 365,640.00 USD (trescientos sesenta y cinco mil seiscientos cuarenta 00/100 dólares americanos), más IVA. Se adjunta al presente informe la propuesta económica del proveedor.

A través de correo electrónico, el 13 de febrero de 2020, se recibió la cotización del proveedor MAINT S.A., por un valor de 717,600.00 USD (setecientos diecisiete mil seiscientos 00/100 dólares americanos), más IVA. Se adjunta al presente informe la propuesta económica del proveedor.

El 03 de febrero de 2020, a través de correo institucional, se solicitó cotización para la contratación SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL, al proveedor EBTEL CIA. LTDA., sin embargo, no se recibió respuesta del proveedor. Se adjunta al presente informe, el correo de constancia.

5. ANALISIS DE LAS COTIZACIONES RECIBIDAS Y DEFINICIÓN DE LA CONVENIENCIA TÉCNICA Y ECONÓMICA PARA LA CONTRATACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL.

CORPORACIÓN FINANCIERA NACIONAL

De acuerdo con las proformas recibidas de CNT E.P. y MAINT S.A. se presenta un cuadro comparativo de los costos finales de las cotizaciones recibidas para el servicio requerido por la CFN B.P., con el fin de determinar el costo de la contratación y establecer el presupuesto referencial.

		OFERENTE 1 CNT E.P.		OFERENTE 2 MAINT S.A.	
Detalle	**Cant.**	**Costo unitario (USD)**	**Subtotal (USD)**	**Costo unitario (USD)**	**Subtotal (USD)**
Servicio de monitoreo y gestión de seguridades que incluye: - Cortafuegos (Firewall) de siguiente generación en un esquema de Alta Disponibilidad (HA) en modo Activo /Pasivo en Quito (24) - Cortafuegos (Firewall) de siguiente generación en un esquema de Alta Disponibilidad (HA) en modo Activo /Pasivo en Guayaquil (24) - Balanceo de carga de enlaces para tráfico saliente (24) - Acceso VPN IPSEC (24) - Acceso VPN SSL (24) - Filtrado de navegación Web con inspección de contenido SSL (24) - Control de Aplicación con mecanismos y firmas para Anti-Bot (24) - Protección contra Intrusos (IPS) (24) - Antivirus Perimetral (24) - Antivirus y Antispam para correo electrónico (24) - Web Application Firewall con protección de contra ataques distribuidos de denegación de servicio (DDOS) a nivel de aplicación (24) - Sistema de emulación de incidentes de seguridad (SandBoxing) (24) - Licenciamiento - Sistema de analítica y manejo avanzado de reportes - Monitoreo Proactivo - SOC - Administración compartida - Servicio de instalación y configuración - Mantenimiento Preventivo (1 vez al año) - Mantenimiento correctivo (24x7) - Transferencia de conocimientos	24	15,235.00	365,640.00	29,900.00	717,600.00
Subtotal		**15,235.00**	**365,640.00**	**29,900.00**	**717,600.00**
IVA (12%):		-	43,876.80	-	86,112.00
Total		-	**409,516.80**	-	**803,3712.00**

De las cotizaciones recibidas, se puede observar que la mejor propuesta económica es la presentada por el valor de 365,640.00 USD (trescientos sesenta y cinco mil seiscientos cuarenta 00/100 dólares americanos), más IVA, siendo la más conveniente a los intereses institucionales.

Adicionalmente se debe indicar que se facilitó a los oferentes los términos de referencia que contienen los requisitos mínimos para la presente contratación para que puedan emitir sus cotizaciones.

En consecuencia con lo anteriormente expuesto y toda vez que se ha determinado que existe la conveniencia y viabilidad técnica para la contratación del **SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL**, mediante proceso de Contratación Interadministrativa con el Oferente 1 (Corporación Nacional de Telecomunicaciones CNT E.P.), y dado que en la propuesta remitida por dicho proveedor se consideran los aspectos técnicos requeridos por la institución y existe la conveniencia económica al ser la propuesta de menor valor, se recomienda acoger dicho presupuesto que servirá para definir el presupuesto referencial del presente proceso de contratación.

CORPORACIÓN FINANCIERA NACIONAL

6. CONCLUSIÓN

Por los antecedentes expuestos, con fundamento en lo establecido en el artículo 105, numeral 2 y 3, del Reglamento Interno de Contrataciones de la Corporación Financiera Nacional B.P., existiendo la respectiva conveniencia y viabilidad técnica y económica, se recomienda invitar a la empresa pública Corporación Nacional de Telecomunicaciones CNT E.P. con RUC 1768152560001 , a participar en el proceso de Contratación Interadministrativo para la contratación del **SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL**, con un presupuesto de 365,640.00 USD (trescientos sesenta y cinco mil seiscientos cuarenta 00/100 dólares americanos), más IVA.

Elaborado por:	Revisado por:
Ing. Andrea Rodríguez Fierro **Ingeniera de servidores y sistemas operativos 2**	Ing. Carlos Coba Cisneros **Especialista en Gestión de Proyectos Informáticos**

Aprobado por:
Ing. José Játiva Ubillús **Gerente de Tecnologías de la Información**