CORPORACIÓN FINANCIERA NACIONAL

CORPORACIÓN FINANCIERA NACIONAL B.P.

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL

Marzo, 2020

CORPORACIÓN FINANCIERA NACIONAL

Contenido

1. ANTECEDENTES Y JUSTIFICACIÓN 3
2. OBJETO DE LA CONTRATACIÓN 5
3. OBJETIVOS ESPECIFICOS 5
4. ALCANCE 6
5. METOLOGÍA DE TRABAJO Y REQUERIMIENTOS POR GESTIÓN DE RIESGO OPERATIVO (CONFORME A LAS DISPOSICIONES DE LA SUPERINTENDENCIA DE BANCOS): 6
6. INFORMACIÓN QUE DISPONE LA ENTIDAD 11
7. PRODUCTOS O SERVICIOS ESPERADOS 13
8. ESPECIFICACIONES TÉCNICAS 15
8.1. SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO PREVENTIVO 28
8.2. SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO CORRECTIVO 28
8.3. SERVICIO DE SOPORTE TÉCNICO Y ACTUALIZACIONES 29
8.4. SERVICIOS DE INSTALACIÓN Y CONFIGURACIÓN 29
8.5. OTROS SERVICIOS ESPECIALIZADOS 30
8.5.1. Servicios de Contingencias 30
8.5.2. Servicios de Monitoreo Proactivo 31
9. ENTREGABLES 31
10. PLAZO TOTAL DE LA CONTRATACIÓN 32
11. FORMA DE PAGO 32
12. OBLIGACIONES DEL CONTRATANTE 33
13. OBLIGACIONES DEL CONTRATISTA 33
14. GARANTÍAS 33
15. MULTAS 33
16. LOCALIDAD 35

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DEL DELSERVICIO 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

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,

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

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;

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

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.

2. OBJETO DE LA CONTRATACIÓN

SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL

3. OBJETIVOS ESPECIFICOS

- Cumplir con la normativa y recomendaciones de los organismos de control
- Garantizar la seguridad, disponibilidad y rendimiento de los servicios que la CFN B.P. provee.
- Mantener la información de la CFN B.P. protegida mediante controles de seguridad perimetral.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

4. ALCANCE

La CFN B.P. al ser una entidad financiera pública, para cumplir con los organismos de control y velar por la seguridad de la información que maneja la institución, requiere mantener un Servicio de Seguridad Perimetral Gerenciada acogiendo buenas prácticas internacionales en la prestación del servicio y así garantizar su eficiencia.

La plataforma de Seguridad Perimetral Gerenciada que requiere la CFN B.P está basada en un esquema geográfico de alta disponibilidad (HA) con un esquema Activo/Activo –Activo/Pasivo para los centros de datos de la ciudad de Guayaquil y Quito, la activación del Firewall de tercera generación, VPN IPSEC, VPN SSL, Filtrado de navegación Web, Control de Aplicaciones, Protección contra Intrusos (IPS), Antivirus, Balanceo de Aplicaciones, Anti Bot, funciones de red avanzadas (QoS), Sandboxing se brindarán mediante appliance de propósito específico, los servicios de Antivirus y Antispam para correo electrónico, Web Application Firewall, protección contra ataque DDoS, se brindarán desde la periferia desde la infraestructura del proveedor.

Así también, el servicio debe proveer de un sistema de monitoreo proactivo, mantener un Centro de Operaciones de Seguridad (Security Operations Center) SOC y manejar una data de hasta un año de generada la información, para análisis y reportes que faciliten la gestión y haga visibles los incidentes de seguridad que se presentan en el perímetro de la red de la CFN B.P.; esto con la finalidad de mejorar el servicio actual con el que se cuenta, en la que se depende absolutamente de las capacidades del ISP.

5. METOLOGÍA DE TRABAJO Y REQUERIMIENTOS POR GESTIÓN DE RIESGO OPERATIVO (CONFORME A LAS DISPOSICIONES DE LA SUPERINTENDENCIA DE BANCOS):

5.1. METODOLOGÍA DE TRABAJO

Para la prestación del servicio, la metodología de trabajo contempla los siguientes aspectos:

- Se implementará en los centros de datos de la ciudad de Guayaquil y Quito.
- Dentro de los primeros 15 días de vigencia del contrato, el proveedor deberá realizará la actualización de licencias y afinamiento en la plataforma.
- Se realizará dos pruebas globales durante la vigencia del contrato (una por año), sobre la operatividad y el funcionamiento de la plataforma de seguridad perimetral y su esquena de alta disponibilidad, orientadas a dar cumplimiento al Plan de Continuidad del Negocio y Recuperación de Desastres de la Institución. Por la realización de estas pruebas, la CFN B.P. no deberá incurrir en gastos adicionales.
- La administración de la plataforma será compartida, es decir el personal técnico de la Gerencia de Tecnología de la Información, designado para el efecto y comunicado al proveedor por parte del Administrador del contrato, de acuerdo con las necesidades, podrá ejecutar cambios en la infraestructura.
- Las tareas de mantenimiento preventivo y actualizaciones serán efectuadas en las oficinas de la CFN B.P., en las ciudades de Guayaquil y Quito
- Para las actividades de migración y actualización de versiones o actividades que tengan impacto o suspensión del servicio que brinda la plataforma, la CFN B.P. establecerá los horarios para su ejecución, pudiendo ser horarios no laborables, incluyendo fines de semana y días festivos.
- Toda la documentación estará sujeta a la metodología de proyectos de la Gerencia de Tecnología de la Información de la CFN B.P.; dentro de los primeros 15 días de suscripción del contrato, se realizará la entrega por parte de CFN B.P al Supervisor del contrato del contratista.
- Para la comunicación y atención de los incidentes reportados por la CFN B.P. se utilizará como canal de ingreso de incidentes o requerimientos el Centro de soporte del proveedor (mesa de servicios); y, como mecanismo opcional para reportar incidentes las siguientes opciones:
    - Llamadas telefónicas y/o mensajes de texto

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

- Mensajes de correo electrónico

5.2. 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, el contratista durante la ejecución del contrato deberá cumplir con lo establecido en los acuerdos que se detallan a continuación:

5.2.1. Acuerdo de Nivel de Servicio (SLA)

El contratista de acuerdo a lo señalado 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 GESTION DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral 14, literal b, i: "*Niveles mínimos de calidad del servicio acordado*", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, deberá incluir en su oferta un "ACUERDO DE NIVEL DE SERVICIO" suscrito por el contratista, donde se estipule como mínimo lo siguiente:

Mecanismos activos de protección	**Nivel de disponibilidad Solicitado (%)**
Cortafuegos (Firewall) de siguiente generación en un esquema de Alta Disponibilidad (HA) en modo Activo /Pasivo, tanto en Quito como en Guayaquil.	99,80%
Balanceo de carga de enlaces para tráfico saliente	99,80%
Acceso VPN IPSEC, VPN SSL	99,80%
Filtrado de navegación Web con inspección de contenido SSL	99,80%
Control de Aplicación con mecanismos y firmas para Anti-Bot	99,80%
Protección contra Intrusos (IPS)	99,80%
Antivirus Perimetral	99,80%
Antivirus y Antispam para correo electrónico	99,90%
Web Application Firewall con protección de contra ataques distribuidos de denegación de servicio (DDOS) a nivel de aplicación.	99,90%
Componentes de Control y Administración	**Nivel de disponibilidad Solicitado (%)**
Sistema de Analítica y Manejo avanzado de Reportes	99,80%
Sistemas de Emulación de Incidentes de Seguridad (sandboxing)	99,90%

- Periodo de Evaluación: Mensual.

  Los tiempos de indisponibilidad del servicio serán contabilizados desde el momento de notificación del incidente al Centro de soporte del proveedor

Esquema de atención:

La atención requerida para Cambios e Incidentes que pueden ocurrir durante la prestación del servicio deberá considerar los siguientes requerimientos mínimos.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Gestión de Cambios:

Descripción	Respuesta inicial	Tiempo de ejecución
Cambios sobre módulos gestionados por el proveedor: configuraciones de software base (firmware), configuraciones de alta disponibilidad, configuraciones de gestión y configuraciones de red.	4 horas a partir de la notificación en el Centro de soporte del proveedor	Hasta 24 de horas de ejecución contra conformidad de CFN B.P.
Consultas generales que el personal de CFN B.P. requiera sobre la validez de una configuración sobre módulos que contemplen administración compartida.	4 horas a partir de la notificación en el Centro de soporte del proveedor	Hasta 24 de horas de ejecución contra conformidad de CFN B.P.
Asistencia y acompañamiento en cambios sobre todas las funcionalidades del servicio: módulos con gestión compartida y módulos con gestión del proveedor.	4 horas a partir de la notificación en el Centro de soporte del proveedor	Deberá ser dentro de 48 Horas, después de que CFN B.P. lo solicite al centro de soporte del proveedor.

Gestión de Incidentes:

Prioridades de atención y resolución de Incidentes:

- **Prioridad Alta:** Cuando el servicio o equipo se encuentre caído lo cual impacta a la disponibilidad. El tiempo máximo transcurrido desde el reporte del incidente hasta su resolución es de 1 hora. El proveedor deberá mantener informado al contratante cada cuatro (4) horas hasta la estabilización del servicio durante las siguientes 72 horas de reportado el incidente, que será el tiempo máximo para cerrarlo.

- **Prioridad Media:** Cuando se tenga una degradación en el servicio; pero está aún no afecta la disponibilidad del servicio o equipo. El tiempo máximo transcurrido desde el reporte del incidente hasta su resolución es de 2 horas. El proveedor deberá mantener informado al contratante cada ocho (8) horas hasta la estabilización del servicio durante las siguientes 72 horas de reportado el incidente, que será el tiempo máximo para cerrarlo.

- **Prioridad Baja:** Cuando no hay afectación a la disponibilidad del servicio o no hay degradación del servicio, pero se requiere ejecutar un mantenimiento. El tiempo máximo transcurrido desde el reporte del incidente hasta su resolución es de 8 horas. El proveedor deberá mantener informado al contratante cada día hasta la estabilización del servicio durante las siguientes 72 horas de reportado el incidente, que será el tiempo máximo para cerrarlo.

Tiempo de resolución en caso de necesitar cambio de partes o piezas:

- Una vez determinado el diagnóstico del daño por parte del proveedor, el tiempo máximo para solución para el reemplazo de partes o piezas es "Siguiente Día Calendario". Entendiendo que la reparación incluye las siguientes actividades: identificación de la causa, acciones correctivas y el restablecimiento del estado normal de operatividad; es decir, que el problema detectado haya sido resuelto en su totalidad.

Niveles de escalamiento:

- **Primer nivel:** Mediante atención telefónica o correo electrónico; la CFN B.P. realizará el seguimiento respectivo del caso reportado

- **Segundo nivel:** El contratista deberá proporcionar soporte local en sitio; para ello, el contratista deberá contar con técnicos certificados para clarificar, aislar y resolver problemas relacionados con la infraestructura objeto del proceso de contratación

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

- **Tercer nivel:** Cuando sea requerido, el contratista, escalará el caso al siguiente nivel de soporte en un Centro Internacional de Soporte Técnico del fabricante. El número de caso asignado por el Centro Internacional de Soporte Técnico del fabricante deberá ser proporcionado al cliente para efectos de seguimiento, y será obligación del Contratista mantener informados del estado/progreso en la resolución del caso, a los técnicos del cliente.

Penalizaciones:

- En caso de existir incumplimiento en los tiempos de atención o resolución de incidentes, definidos en el SLA, la contratante descontará de los pagos mensuales los valores que correspondan.
- Los costos asociados al incumplimiento de la disponibilidad de cada uno de los servicios se calcularán de acuerdo a la tabla indicada en la sección de multas.

5.2.2. 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, el contratista deberá cumplir con lo establecido en el **"ACUERDO DE TRANSFERENCIA DE CONOCIMIENTOS"**, cuyo formulario deberá ser presentado como parte de su oferta.

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

- Brindar una transferencia de conocimientos basada en la administración de los equipos bajo el esquema solicitado de administración compartida, por lo cual deberá ser interactiva, exponiendo las limitaciones de los permisos asignados al personal de la Gerencia de Tecnología de la Información.
- La transferencia de conocimientos se deberá realizar dentro del primer trimestre contado a partir de la suscripción del contrato.
- La transferencia de conocimientos se la realizará como mínimo a 6 funcionarios de la CFN B.P indicados por el Administrador del contrato, está se brindará en las instalaciones del contratista en la ciudad de Quito, deberá tener un mínimo de 20 horas y debe incluir el material didáctico y físico emitido a los participantes.
- La transferencia de conocimientos debe ser realizada por el personal capacitado y calificado del contratista 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, el Contratista deberá entregar certificados de participación, el mismo que debe contener: tema, número de horas de duración, nombre del instructor con su firma y sello de la empresa contratista y deberá ser entregado, máximo a los 3 días posteriores a la realización de dicha trasferencia.
- La trasferencia de conocimientos no tendrá costo adicional para la CFN B.P.

5.2.3. 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, el Contratista deberá cumplir con lo establecido en el **"ACUERDO DE CONFIDENCIALIDAD DE INFORMACIÓN Y DATOS"**, cuyo formulario deberá ser presentado como parte de su oferta.

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

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

- Será responsabilidad del 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.

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

- El 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.

- El 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.

- El 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.

5.2.4. 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, el Contratista deberá cumplir con lo establecido en el **"ACUERDO DE PROPIEDAD INTELECTUAL"**, cuyo formulario deberá ser presentado como parte de 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.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

5.2.5. ACUERDO DEL EQUIPO DE TRABAJO Y SUPERVISOR DEL CONTRATISTA

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 contratista", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, el contratista deberá cumplir con lo establecido en el **"ACUERDO DEL EQUIPO DE TRABAJO Y ADMINISTRADOR/SUPERVISOR DEL CONTRATO"**, cuyo formulario deberá ser presentado como parte de su oferta.

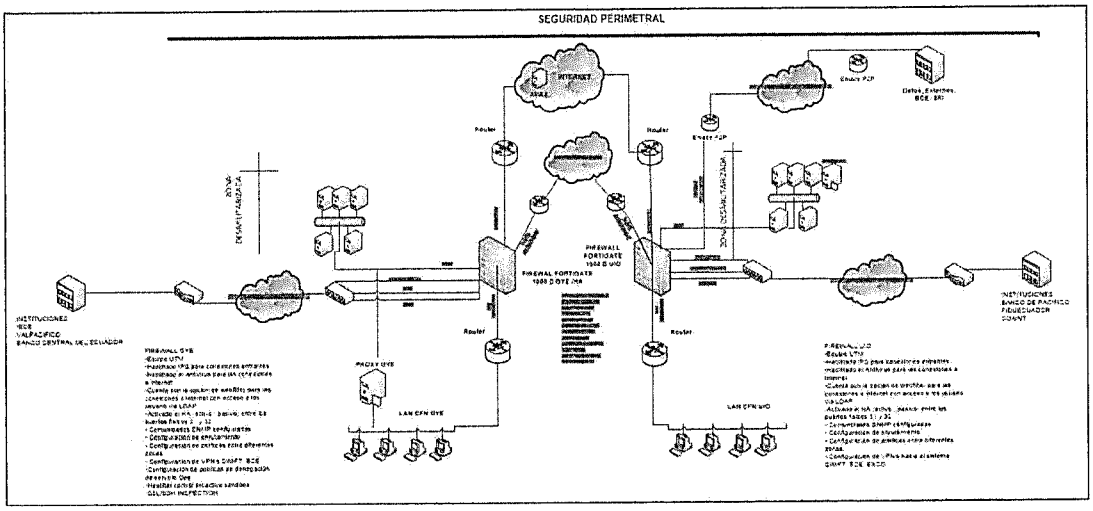
En el acuerdo del equipo de trabajo del contratista se incluye como mínimo las siguientes obligaciones:

- Designar un supervisor de contrato
- Definir un arquitecto de solución
- Definir dos ingenieros especializados en seguridades

6. INFORMACIÓN QUE DISPONE LA ENTIDAD.

La Corporación Financiera Nacional B.P., dispone actualmente de los siguientes servicios que forman parte de la plataforma de Seguridad Gerenciada:

Ilustración 1: Arquitectura de Seguridad Gerenciada a Nivel Nacional



Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Ilustración 2: Arquitectura de Seguridad Gerenciada - CFN Quito

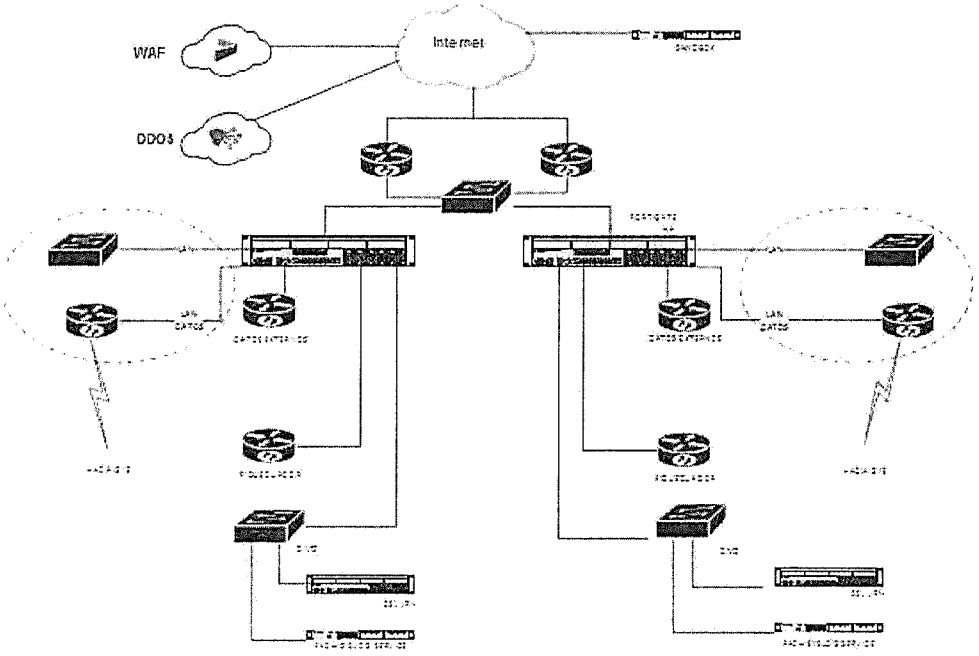
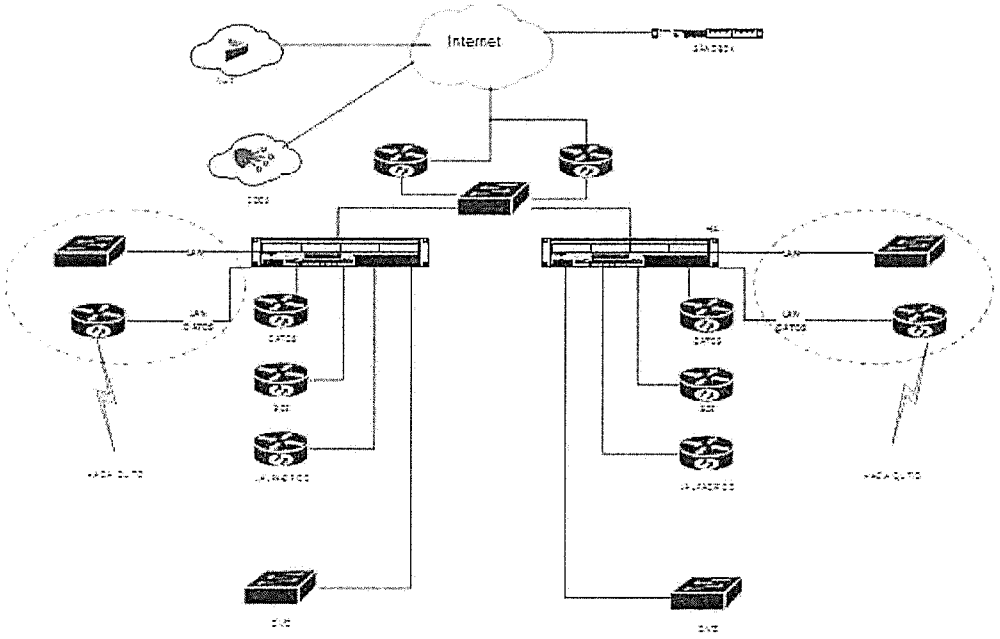


Ilustración 3: Arquitectura de Seguridad Gerenciada -CFN Guayaquil

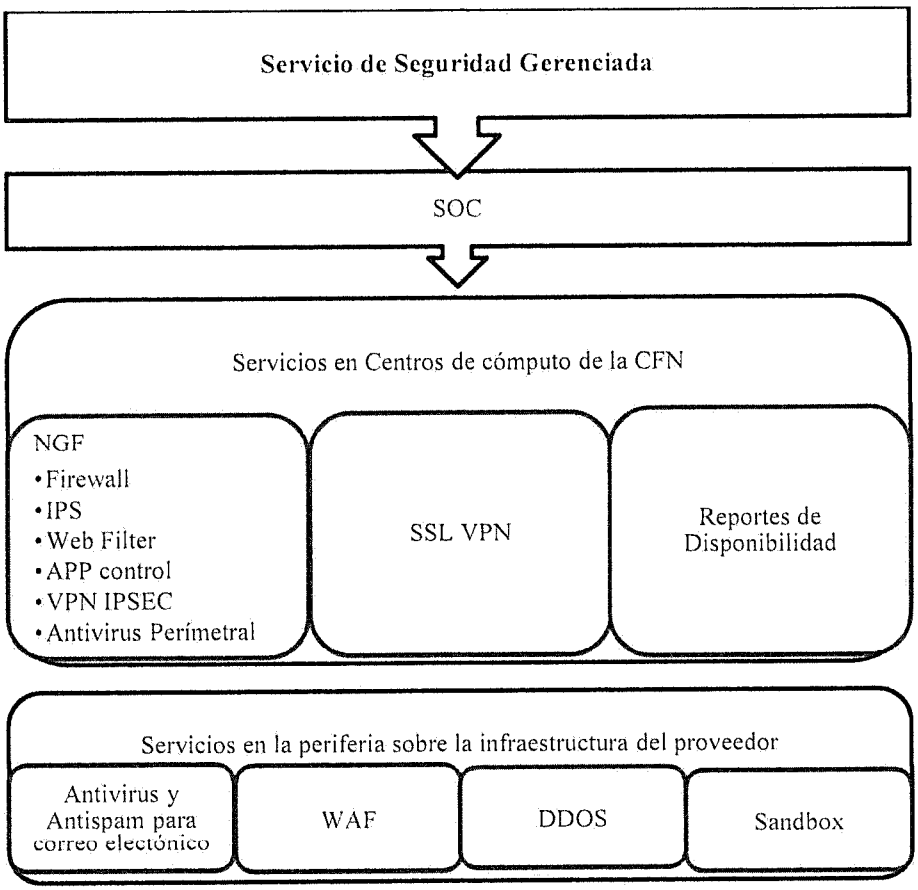


Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Tabla 1: Localidades de CFN para el despliegue del servicio

Oficina - Localidad	Dirección
Quito	Calle Iñaquito 36 A, entre Corea y Av. Naciones Unidas, Edificio Platinum G, piso 6
Guayaquil	Av. 9 de Octubre y Pichincha, Edificio del Banco Central de Ecuador, Piso 1

Ilustración 1: Servicios Requeridos de Seguridad Gerenciada



7. PRODUCTOS O SERVICIOS ESPERADOS

La CNF 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:

7.1 Los mecanismos activos de protección 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

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

- 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.

7.2 Los componentes de control y administración son los siguientes:

- Sistema de analítica y manejo avanzado de reportes, que mediante correlación de registros de seguridad (Security Logs) facilite la gestión y evidencie 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 dichos incidentes.

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

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

8. ESPECIFICACIONES TÉCNICAS

El servicio de Seguridad Gerenciada deberá cumplir con las siguientes especificaciones técnicas:

#	ESPECIFICACIONES TECNICAS SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA
1	CARACTERÍSTICAS GENERALES DE LOS SERVICIOS REQUERIDOS
1.1	Se requiere de un modelo de administración compartida entre el proveedor y el cliente.
1.2	El personal técnico de CFN B.P. contará con privilegios administrativos para realizar la gestión parcial de políticas de firewall y perfiles de seguridad. Esto incluye perfiles de Filtrador de Navegación, Control de Aplicación, IPS, Antivirus perimetral.
1.3	El cliente contará con privilegios de lectura para los componentes de: SSL VPN, Web Application Firewall, Antivirus y Antispam para correo electrónico, sistema de analítica y manejo de reportes y sistema para emulación de incidentes de seguridad (Sandboxing).
1.4	El proveedor será responsable de la disponibilidad de la plataforma de seguridad en esta modalidad.
1.5	El proveedor será responsable de configurar y mantener los parámetros de funcionamiento adecuado para garantizar la disponibilidad.
1.6	El proveedor realizará monitoreo de disponibilidad y backups de los componentes del servicio de seguridad.
1.7	El proveedor garantizará la continuidad tecnológica de la solución de seguridad dentro del ciclo de vida del contrato.
1.8	El servicio deberá considerar la Gestión del Cambio "Change Management" del ciclo de vida de la solución de seguridad.
1.9	El servicio deberá considerar la Gestión de Incidentes "Incident Management" del ciclo de vida de la solución de seguridad.
1.10	El proveedor será responsable de realizar la actualización de firmware anualmente de todos los componentes de la solución en caso de ser necesario. Es responsabilidad del proveedor utilizar firmwares que estén probados y homologados para funcionalidades que requiere CFN B.P.
1.11	Es responsabilidad del proveedor realizar un monitoreo de disponibilidad de la solución de seguridad.
1.12	El proveedor deberá contar con un Centro de Operaciones de Seguridad - SOC con operación 24X7X365.
1.13	La entrega de los servicios de: Firewall, Filtrado de navegación Web, IPS, Antivirus, Control de Aplicaciones y VPN SSL y IPSEC deberá ser realizada mediante hardware de propósito específico que cubran este conjunto de funcionalidades y que sean de última generación.
1.14	La entrega del Sistema de emulación de incidentes de seguridad (Sandboxing) deberá ser entregada mediante hardware de propósito específico que cubran estas funcionalidades o mediante servicios implementados en la infraestructura del proveedor.
1.15	Los servicios de protección para correos de Antivirus y AntiSpam, así como de WAF/DDOS deben ser implementados en la infraestructura del proveedor.
1.16	Soporte clúster HA para servicio de Firewall, Filtrado de navegación Web, IPS, Control de Aplicaciones, IPSEC.
1.17	La solución deberá contar con la opción de resolver los sistemas de nombre de dominio (DNS) a través de direcciones IP públicas del proveedor.
1.18	La capacidad de que el firewall pueda discriminar el tráfico de salida hacia Internet a través de sus interfaces.
1.19	Por ser un servicio critico que afecta todo el desenvolvimiento del negocio a nivel nacional, la contratista deberá garantizar la disponibilidad del servicio.
1.20	CFN B.P., requiere durante la vigencia del contrato, que el proveedor este en la capacidad de ejecutar procesos de reingeniería y re-implementación de la solución de seguridades de acuerdo a las necesidades tecnológicas y de procesos de la contratante, el cual no tendrá costo para la institución.
1.21	El oferente deberá garantizar el servicio técnico en la ciudad de Quito y Guayaquil para brindar mantenimiento de la solución ofertada y garantizar el SLA de cada servicio. Dependiendo de la

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

	necesidad deberá ser presencial o virtual; se debe contar con un técnico en Quito que atienda a la ciudad de Quito y uno en Guayaquil que atienda a la ciudad de Guayaquil.

2	LAS CARACTERÍSTICAS MÍNIMAS QUE SE DEBEN CUMPLIR PARA BRINDAR EL SERVICIO DE FIREWALL SON:
2.1	El responsable técnico de la CFN B.P. contará con la potestad de acceder y modificar los parámetros básicos de los apartados de configuración que se citan a continuación: ▪ configuración de usuarios, ▪ configuración de las funcionalidades de reglas de firewall, ▪ configuración de los perfiles de antivirus, ▪ configuración de perfiles para protección de intrusos (IPS), ▪ configuración de perfiles de filtrado web, ▪ configuración de perfiles para control de aplicaciones. La gestión de estos componentes será responsabilidad CFN B.P.
2.2	El responsable técnico de CFN B.P., podrá acceder a las configuraciones previamente mencionadas, una vez que el proveedor haya finalizado la entrega del servicio a conformidad de CFN B.P.
2.3	El proveedor será responsable de la gestión de cambios avanzados sobre el firewall y la gestión de incidentes correspondiente.
2.4	El proveedor será responsable de gestionar cualquier incidente de hardware o software con el respectivo fabricante de los equipos provistos para la entrega de los servicios cuando así lo amerite.
2.5	Manejar políticas independientes para diferentes flujos de tráficos, que sean establecidos o configurados en la solución.
2.6	El servicio firewall deberá estar en la capacidad de procesar la información con un mínimo de 20000 sesiones concurrentes por hora, que es el número de sesiones promedio que actualmente se consume.
2.7	Soporta conexiones con alto rendimiento.
2.8	Al pertenecer al tipo de última generación (NGFW) su capacidad de procesamiento mínimo debe ser de 5 Gbps.
2.9	La capacidad para procesar información debe ser: ▪ para el sistema de prevención de intrusos al menos debe ser de 6 Gbps, ▪ en lo que respecta al sistema para la prevención de amenazas, al menos 3.6 Gbps y ▪ en cuanto al sistema de VPN-SSL de al menos 3 Gbps, En caso de incrementar la información durante la vigencia del contrato deberá ser capaz de ser superados estos valores.
2.10	El hardware para el servicio de Firewall deberá contar como mínimo con una capacidad de 16 GB de RAM o superior, con al menos 12 Interfaces físicas 10/100/1000 Mbps RJ45, para poder brindar los servicios requeridos, considerando HA y el crecimiento de la solución durante la duración de los servicios.
2.11	El servicio firewall deberá permitir ser administrable vía WEB (HTTPS) y SSH.
2.12	Visualización gráfica de dashboard en el panel de control.
2.13	Soporte y conexiones para alta disponibilidad o clúster.
2.14	Conexiones a la red WAN.
2.15	Realizar balanceo de carga de tráfico saliente.
2.16	Tener la capacidad en modo comando de revisar la configuración total que soporta el servicio.
2.17	Actualizaciones automatizadas de patrones (antivirus, IPS, etc.).
2.18	En la solución se podrá visualizar el estado y fecha de vigencia de las licencias que cuenta en la herramienta.
2.19	Deberá permitir la configuración de perfiles de escaneo de virus en sentido saliente.
2.20	Notificación de alarmas y eventos por correo electrónico y SNMP.
2.21	Opciones programables de restauración y copia de seguridad.
2.22	La solución podrá ser configurada mediante scripts automáticos para que realice un backup de la configuración a un servidor SFTP, FTP o TFTP de manera semanal.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

2.23	Soporte de contraseña tipo OTP.
2.24	Debe tener doble factor de autenticación compatible con Entrust Security Guard.
2.25	Las reglas de firewall deben analizar las conexiones que atraviesan la solución planteada, entre interfaces, grupos de interfaces y VLANs.
2.26	Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta fuente y destino.
2.27	Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
2.28	Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo.
2.29	Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
2.30	Capacidad de hacer traslación de direcciones estático, uno a uno, NAT, NAT destino/origen.
2.31	Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
2.32	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, interface línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).
2.33	Deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios.
2.34	Deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN.
2.35	La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada.
2.36	Autenticación a nivel de usuarios, basadas en local database, LDAP, RADIUS, Novell eDirectory y Directorio Activo.
2.37	La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada.
2.38	El dispositivo de seguridad deberá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas.
2.39	La solución podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política.
2.40	El servicio de seguridad perimetral será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.
2.41	El dispositivo podrá generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS.
2.42	La solución deberá ser capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
2.43	El dispositivo integrará la inspección de tráfico tipo SSL y bajo perfiles predefinidos o personalizados.
2.44	El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo qué certificado será válido este tráfico.
2.45	La solución de seguridad perimetral deberá gestionar el inicio de sesión único de usuario integrándose al directorio activo institucional.
2.46	Permitir el uso de autoridades certificadas internas y externas (CA).
2.47	El servicio de seguridad gerenciada deberá incluir la visualización de tráfico y conexiones WAN.
2.48	Establecer pesos a cada conexión WAN.
2.49	Control de Acceso, permisos a usuario para acceso a la administración.
2.50	Soporte para protección avanzadas contra amenazas.
2.51	Inspección de tráfico TCP y UDP.
2.52	Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSL dentro de todos o cierto rango de puertos configurados para este análisis.
2.53	Contar con el servicio de protección avanzada proactiva Sandboxing.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

2.54	Deberá contar con un IPS integrado y crear firmas dentro de la solución de seguridad.
2.55	Prevención de todas las amenazas, tanto conocidas como desconocidas.
2.56	Integración de usuarios en las políticas, no solo de direcciones IP.
2.57	La solución deberá implementar políticas para prevenir ataques de denegación de servicio (DoS).
2.58	Capacidad de poder garantizar ancho de banda en el servicio de seguridad perimetral.
2.59	Capacidad de poder definir límite de ancho de banda (ancho de banda máximo).
2.60	Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.
2.61	Capacidad de poder definir calidad de servicio al tráfico de voz sobre IP y Videoconferencia.
2.62	Servicio de Firewall perimetral para CFN B.P. Quito y Guayaquil.
2.63	El proveedor deberá incluir soporte para configuración de políticas 7X24x365 días laborables y soporte técnico para incidentes de 24x7x365 días al año para atención de problemas e incidentes.
2.64	El proveedor deberá monitorear el servicio y deberá realizarse por medio de consolas centralizadas en un Centro de Operaciones de Seguridad.
2.65	El proveedor deberá incluir la facilidad de soporte local para los casos que el incidente amerite, con técnicos especialistas en seguridades y con conocimiento de las soluciones instaladas.
2.66	La solución deberá contemplar en cada sitio una configuración de Firewall en Alta Disponibilidad Activo/Activo o Activo/Pasivo de acuerdo con las necesidades de la CFN B.P.
2.67	**ALTA DISPONIBILIDAD**
2.67.1	El NGF deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6.
2.67.2	Alta Disponibilidad en modo Activo-Pasivo.
2.67.3	Alta Disponibilidad en modo Activo-Activo (En el caso que se solicite).
2.67.4	Posibilidad de definir al menos dos interfaces para sincronía.
2.67.5	El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red.

3	SERVICIO DE CONECTIVIDAD Y SISTEMA DE RUTEO
3.1	Soporte a etiquetas de VLAN (802.1q).
3.2	Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
3.3	Soporte a políticas de ruteo (policy routing).
3.4	El soporte a políticas de ruteo deberá permitir que, ante la presencia de dos enlaces a Internet, se pueda decidir que tráfico sale por un enlace y qué tráfico sale por otro enlace.
3.5	Soporte a ruteo dinámico OSPF, BGP, IBGP.
3.6	La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.
3.7	Soporte a ruteo de Multicast.
3.8	La solución deberá permitir la integración a través de Syslog.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

3.9	La solución podrá habilitar políticas de ruteo en IPv6.
3.10	La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6.
3.11	La solución deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, y por usuario, con IPv6.
3.12	La solución deberá habilitar funcionalidades de Firewall de Nueva Generación (Antivirus, Filtrado Web, Web Application Control, Control de Aplicaciones, IPS, Filtrado de correo, Sandboxing) dentro de las políticas creadas con direccionamiento IPV4 y soportarlo para IPv6.
3.13	El dispositivo debe integrar la autenticación por usuario en IPv6.
3.14	El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explícito.
3.15	La solución podrá restringir direcciones IPv6 en modo proxy explícito.
3.16	Deberá hacer NAT de la red en IPv6.
3.17	Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo.
3.18	La solución deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Sandboxing, Antivirus, para la inspección de tráfico en IPv6 basado en flujos.
3.19	La solución deberá contar con una base de administración de información interna generada por sesiones sobre IPv6.
3.20	La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad.
3.21	El dispositivo podrá hacer la función como servidor DHCP IPv6.

4	CARACTERÍSTICAS DE SERVICIO VPN IPSEC/L2TP/PPTP
4.1	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
4.2	Soporte para IKEv2 y IKE Configuration Method.
4.3	Debe soportar la configuración de túneles PPTP.
4.4	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
4.5	Se debe soportar longitudes de llave para AES de 128 y 256 bits.
4.6	Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
4.7	Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256, SHA512.
4.8	Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSec site-to-site y VPNs IPSec client-to-site.
4.9	Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

4.10	El SLA (acuerdo de niveles de servicio) deberá ser de un 99.8%de disponibilidad correspondiente al servicio de VPN IPSEC/L2TP/PPTP.

5	SERVICIO FILTRADO DE URLS (URL FILTERING)
5.1	Facilidad para incorporar control de sitios a los cuales navegan los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y más de 35 millones de sitios web en la base de datos.
5.2	Debe poder categorizar contenido Web requerido mediante IPv6.
5.3	El servicio debe permitir el escaneo en tiempo real de malware.
5.4	Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de la fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
5.5	La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo).
5.6	Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de reemplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo.
5.7	Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido.
5.8	Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
5.9	La solución de Filtrado de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.
5.10	Deberá ser posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
5.11	Deberá ser posible exceptuar la inspección de HTTPS por categoría.
5.12	Se debe incluir la funcionalidad de reputación basada en filtrado de URLs, como mínimo deberá manejar los siguientes modos: Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.
5.13	Se debe incluir la funcionalidad de reputación basada en filtrado de URLs.
5.14	El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en tiempo de acceso a las categorías.
5.15	Autenticación remota por medio de una base de datos proporcionada por el Directorio Activo (Microsoft AD, eDirectory).
5.16	Permitir manejo de listas blancas que puedan excluir ciertos filtros de seguridad web.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

6	SERVICIO PROTECCIÓN CONTRA INTRUSOS (IPS)
6.1	El servicio de detección y prevención de intrusos, debe poder implementarse en línea, y el tráfico a ser inspeccionado deberá pasar a través de la infraestructura dedicada para la solución ofertada.
6.2	Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.
6.3	Capacidad de detección de más de 4000 firmas en constante actualización
6.4	Capacidad de actualización automática de firmas IPS.
6.5	Identificar y bloquear sondeos y ataques relacionados con aplicaciones y protocolos mediante inspección profunda de paquetes.
6.6	La detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signaturebased/ misusedetection).
6.7	Basado en análisis de firmas en el flujo de datos en la red, deberá permitir configurar firmas nuevas para cualquier protocolo.
6.8	Deberá contar con el bloqueo de tráfico dirigido a servidores de comando y control, y redes de bots.
6.9	El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
6.10	Sondeos, escaneos de puertos, interrogaciones, host sweeps
6.11	Protección contra flood: SYN TCP, UDP, ICMP.
6.12	En caso de que haya eventos que comprometan la seguridad de la institución el proveedor deberá enviar Alertas vía correo electrónico.
6.13	Prevenir violación de protocolos.
6.14	Protección de amenazas día-cero.

7	SERVICIO DE INSPECCIÓN DE CONTENIDO SSL
7.1	La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
7.2	La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
7.3	La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

7.4	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
7.5	Debe de analizar contenido cifrado SSL para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.

8	SERVICIO DE VPN SSL
8.1	El servicio de acceso VPN SSL deberá proporcionar una conexión segura entre los usuarios remotos y los recursos de la red interna de CFN B.P.
8.2	El servicio deberá permitir una capacidad mínima de 25 conexiones concurrentes y no debe tener restricción en el número de usuarios, deberá permitir el despliegue de la solución en HA.
8.3	El servicio de VPN SSL deberá ser de uso dedicado para garantizar el rendimiento de la solución ofertada y de los accesos VPN SSL de los usuarios concurrentes.
8.4	Las VPNs SSL podrán ser accedidas por, laptops, PCs, smartphones, tablets y deberán por lo menos soportar Sistemas Operativos Windows, iOS de Apple, Android.
8.5	El servicio de VPN deberá permitir Múltiple autenticación por usuario con autenticación vía eDirectory y Entrust Identity Guard (servidor radius), Active Directory.
8.6	Deberá ser compatible Entrust Identity Guard (servidor radius) para segundo factor de autenticación de CFN B.P y otros disponibles en el mercado.
8.7	Deberá soportar la encriptación de IPSEC y IKEV2.
8.8	El servicio deberá incluir configuración inicial, soporte y mantenimiento.
8.9	El servicio deberá incluir las actualizaciones necesarias y licenciamiento durante todo el plazo del contrato.
8.10	El proveedor deberá monitorear el servicio VPN SSL desde un SOC (centro de operaciones de seguridad) con personal activo 7x24x365.
8.11	Permitir el monitoreo, mediante el protocolo Simple Network Management Protocol (SNMP), preferible SNMPv3.
8.12	El SLA (acuerdo de niveles de servicio) deberá ser de un 99.8%de disponibilidad para el servicio de VPN SSL.
8.13	El servicio de VPNSSL deberá implementarse con los protocolos de seguridad TLS (Transport Layer Security) versión 1.1 y 1.2.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

9	SERVICIO DE FILTRADO DE CONTENIDO Y CONTROL DE APLICACIONES
9.1	Para proveer el servicio de filtrado de contenido y control de aplicaciones, el proveedor deberá contener el control de acceso de usuarios a páginas WEB no autorizadas y controlar las aplicaciones tipo p2p (edonkey, BitTorrent, skype, etc.).
9.2	El servicio de filtrado de contenido y control de aplicaciones se requiere sea instalado en dos localidades en CFN B.P. Quito y Guayaquil.
9.3	Deberá tener la capacidad manejar por lo menos 50 categorías y una base de por lo menos 19 millones de sitios web personalizables.
9.4	La solución ofertada deberá tener la capacidad de soportar el poder controlar sitios web en más de 5 lenguajes.
9.5	El servicio de filtrado de contenido y control de aplicaciones deberá estar dimensionado y licenciado para mínimo 600 usuarios en CFN B.P. Quito y 600 usuarios en CFN B.P. Guayaquil.
9.6	El servicio de filtrado de contenido y control de aplicaciones deberá filtrar URL por categorías de filtrado, así mismo deberá tener la facilidad de crear perfiles de filtrado para asociar usuarios.
9.7	El servicio de filtrado de contenido y control de aplicaciones deberá permitir agregar listas blancas y listas negras por cada perfil de filtrado.
9.8	El servicio de filtrado de contenido y control de aplicaciones deberá integrarse con el LDAP de Novell con protocolo seguro, que es el software de acceso a la red de CFN B.P.
9.9	El servicio de filtrado de contenido y control de aplicaciones deberá integrarse con el Single Sign-On de Directorio Activo con protocolo seguro, que es el software de acceso a la red de CFN B.P.
9.10	El servicio de filtrado de contenido y control de aplicaciones deberá incluir soporte para modificar la configuración en modalidad 5x8 (días y horas laborables) y soporte para atención de problemas e incidentes en modalidad 24x7x365 (todos los días del año). La CFN B.P. podrá generar inspección en sitio para comprobar este servicio. Replicar para el servicio de firewall y VPN.
9.11	El proveedor deberá monitorear el servicio de filtrado de contenido y control de aplicaciones, éste deberá realizarse por medio de consolas centralizadas en un Centro Especializado en Seguridades Informáticas con personal activo 24x7x365 (todos los días del año). La CFN B.P. podrá generar inspección en sitio para comprobar este servicio. Replicar para el servicio de firewall y VPN.
9.12	El servicio de soporte y actualizaciones será en horario no laborable, para los casos que exista afectación/suspensión del servicio.
9.13	La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
9.14	La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

9.15	La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante de los equipos con los cuales el proveedor brindará el servicio.
9.16	El listado de aplicaciones debe actualizarse periódicamente.
9.17	Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
9.18	Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
9.19	El servicio debe soportar creación de perfiles personalizados donde se incluyan distintos tipos de aplicaciones.

10	ANTIVIRUS Y ANTISPAM PARA CORREO ELECTRÓNICO
10.1	Deberá poseer una gestión del correo electrónico simple a través de una consola de administración unificada a la que se acceda por Internet.
10.2	Todas las funciones de detección, filtrado, cuarentena, copia de seguridad y recuperación deberán ser administradas de manera segura a través del portal habilitado para tal fin.
10.3	Debe filtrar correos no deseados que surgen de correo masivo legítimo bajo la discreción del usuario final.
10.4	Debe permitir habilitar el filtrado de correo electrónico saliente para proteger del malware a los Clientes.
10.5	Debe poder sincronizar la información de su cuenta para usuarios y grupos mediante POP3, IMAP, LDAP, Active Directory.
10.6	Debe poseer como mínimo las siguientes técnicas de detección: spam, virus, spoofing, phishing, spyware, listas negras internacionales (RBL), denegación de servicio.
10.7	Debe permitir configurar por usuario listas blancas y negras, cola de cuarentena, logueo de accesos, estadísticas, cola de emails.
10.8	Debe soportar múltiples dominios
10.9	Debe permitir que los usuarios reciban un email con información de cuarentena.
10.10	Debe manejar el SPAM como mínimo de tres formas diferentes: Cuarentena, Etiquetado, Borrado.
10.11	Debe escalar de manera simple, cuando aumente la cantidad de casillas protegidas.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

10.12	Debe soportar conexiones y relays a nivel de protocolos y servicios de plataforma de correo electrónico. Debe soportar conexiones hacia MTA (Lotus Domino, Sendmail, Exim, Exchange) mediante SMTP y sus variantes y símiles.
10.13	Debe tener la capacidad de realizar análisis de todos los archivos adjuntos y por extensiones.
10.14	Debe soportar análisis de mensajes multimedios (JPG, MP3, etc.).
10.15	Debe tener la capacidad de aplicar reglas de listas negras (blacklist) y listas blancas (whitelist) internas por dominio y por dirección de correo electrónico.
10.16	Debe permitir de acuerdo con los atributos formales, revisar las direcciones del remitente y del receptor, así como la IP del remitente (tener validación SPF (sender policy framework).
10.17	Debe permitir la administración mediante consola, de los servicios, y permitir revisar y configurar los mensajes detectados como spam, que se encuentren en cuarentena, el administrador deberá poder rechazarlos, eliminarlos o aceptarlos.
10.18	Deberá soportar múltiples dominios.

11	SERVICIO DE FIREWALL DE APLICACIONES WEB (WAF)
11.1	Deberá proteger los sitios publicados contra ataques a servicios Web como pueden ser los del tipo SQL injections, de Cross-Site Scripting (XSS) y demás amenazas de las Top 10 catalogadas por la OWASP.
11.2	Se incluye hasta 10 aplicaciones WEB propiedad de CFN B.P. y con un tráfico máximo de 20 Mbps.
11.3	Deberá soportar ataques de DDOS al sitio y realizar Balanceo de Aplicaciones.
11.4	Deberá estar basado en múltiples nodos, a fin de garantizar un SLA mínimo de 99,8% de disponibilidad para el servicio de web application firewall (WAF).
11.5	Seguridad para protocolos HTTP y HTTPS.
11.6	El servicio debe permitir implementar perfiles de seguridad que se ajusten a las especificaciones del negocio.
11.7	Deberá permitir balanceo del tráfico entre al menos 2 servidores remotos diferentes.
11.8	Debe ser capaz de aprender el comportamiento de las aplicaciones y detectar ataques, minimizando el número de falsos positivos.
11.9	Deberá contar con un Dashboard que permita tener estadísticas en tiempo real.
11.10	Deberá brindar una mejora de performance de los sitios protegidos brindando un sistema con características similares a CDN.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

11.11	Protección completa contra ataques de capa 7 tales como DDoS (DistributedDenialofService), SQL injection y el top 10 de ataques OWASP (Open Web Application Security Project).
11.12	Debe enviar notificaciones por correo electrónico en caso de evento, y estar en condiciones de generar un reporte mensual que se envié por el mismo medio.
11.13	Deberá permitir Cache del contenido estático del sitio con el fin de tener un mejor rendimiento, fiabilidad y disponibilidad de los servicios de la CFN B.P., absorbiendo las sobrecargas de tráfico y manteniéndolo en línea.
11.14	Deberá notificar al cliente automáticamente ante eventos considerados sospechosos.
11.15	Debe monitorear las direcciones IP de los servidores Cliente.
11.16	Debe permitir restringir el acceso desde determinados países (geolocalización), así como limitar el acceso de Bots.
11.17	Deberá soportar el manejo de dos direcciones públicas para un mismo servicio (Multiple Origin Servers).
11.18	El contratista será el responsable de cumplir con el licenciamiento adecuado para que las funcionalidades descritas estén habilitadas.

12	ANALÍTICA
12.1	Debe poseer un interfaz web, en donde el contratante podrá acceder con un usuario de lectura a la información consolidada sobre lo que está ocurriendo en su red en materia de seguridad.
12.2	Deberá suministrar reportes tipo ejecutivos resumidos que sean publicados a través de un portal web del proveedor.
12.3	Las capacidades de generación de reportes de la herramienta, debe permitir contar con informes predefinidos que se envíen por correo o estén disponibles de forma online automática de acuerdo a la periodicidad que CFN B.P. requiera
12.4	La solución debe tener un monitoreo centralizado de los componentes activos de protección de Firewall, SSL VPN y Sistema de Emulación de Incidentes de Seguridad.
12.5	La solución debe almacenar los registros (logs) de seguridad de los componentes activos de protección de Firewall, SSL VPN y del Sistema de Emulación de Incidentes de Seguridad
12.6	Se requiere que la herramienta pueda generar alarmas ante determinados eventos.
12.7	Se requiere que la gestión de incidentes para este componente se brinde en modalidad 8x5
12.8	Se requiere que la gestión del cambio para este componente se brinde en modalidad 8x5
12.9	Deberá poder generar reportes de los eventos detectados por el IPS y el antivirus.
12.10	Deberá poder generar reportes de la capacidad del hardware.
12.11	**REPORTES MENSUALES** Los reportes mensuales deberán ser como mínimo los siguientes y estarán sujetos a cambios bajo necesidad y demanda de la contratante:
12.11.1	**Control de Navegación**
	✓ Top de usuarios por consumo de ancho de banda, que contenga: Username, Fuente IP, Ancho de banda, % del subtotal. ✓ Páginas Web con más consumo de ancho de banda

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

	✓ Top por "Categorías permitidas" Ej.: Business, News and Media, Education, Sports, Unknown, lista blanca, etc. ✓ Usuarios que reportan más de una IP como origen de consumo de navegación en internet ✓ Top de usuarios web por tiempo de navegación. ✓ Top de usuarios web por requerimientos, que contenga: Nombre de usuario, página visitada (hostname), # requerimientos (Visitas), % del subtotal (%, en relación con el total de requerimientos)
12.11.2	**Servicio de firewall**
	✓ Top 15 según Origen ✓ Top 15 según Destino ✓ Top 15 Incidentes detectados ✓ Top 10 Puertos atacados por destino ✓ Matriz de correlación entre origen y destino de los ataques (Relación entre orígenes, destinos y firmas de los incidentes)
12.11.12	**Web Application Firewall (WAF)**
	✓ Seguridad: Visitantes de IPs bloqueadas, Visitantes de países bloqueadas, Visitantes a URL bloqueadas, Bot Access Control, Bots Sospechosos, Remote File Inclusion, SQL Injection, Cross Site Scripting, Acceso a recursos ilegales, DDoS,BackdoorProtect ✓ Performance: Ancho de banda Cacheado, Ancho de banda ahorrado por Cache, Pedidos de Cache, Pedidos por Data Center ✓ Generales: Top 5 IPs origen, Top 5 Países, Top 5 Browsers ✓ Tráfico: Pedidos por segundo, Tipo de Browsers, Países, Cantidad de visitas diarias, Visitas por Segundo, Ancho de banda acumulado, Tráfico aceptado/Bloqueado.

13	SISTEMA DE EMULACIÓN DE ATAQUES DE SEGURIDAD (SANDBOXING)
13.1	La solución debe permitir el agregar una capa adicional de control a la plataforma de seguridad de CFN B.P. Debe contar con mecanismos que permitan tener mayor visibilidad de amenazas no detectadas por el antivirus standard.
13.2	La solución debe permitir la conexión del motor de seguridad del firewall hacia el sistema de emulación de ataques de seguridad. Se debe garantizar que la información sospechosa sea analizada en primera instancia por el firewall y posteriormente, sea derivada al ambiente aislado del sistema de emulación de ataques, para poder identificar el comportamiento de la misma.
13.3	La información sospechosa debe ser sometida a un análisis contra una base de datos de seguridad. Si no existe un hash de seguridad relacionado, la información será evaluada por completo por la solución de emulación de ataques de seguridad.
13.4	La solución debe utilizar procesamiento de colas para el análisis de información sospechosa, para garantizar que los tiempos de procesamiento sean los adecuados.
13.5	La solución deberá tomar en cuenta que CFN utiliza los siguientes sistemas operativos: Windows, Linux, Solaris.
13.6	La solución deberá soportar las siguientes técnicas de antievasión: llamadas latentes (Sleep Calls) y consultas de procesos y registro (Process and Registry queries).

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

13.7	La solución deberá detectar las siguientes respuestas a llamadas (CallBack Detection): redirección a URLs maliciosas (malicious URL visit), comunicación con Botnets y redes de comando y control y tráfico generado por software malicioso (malware).
13.8	La solución debe soportar los siguientes formatos de archivos: .7z, .ace, .apk, .arj, .bat, .bz2, .cab, .cmd, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html, .jar, .js, .kgb, .lnk, .lzh, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
13.9	La solución debe interactuar con los siguientes protocolos: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM.
13.10	La solución debe tener al menos la capacidad de análisis de 5000 archivos por hora.
13.11	Se requiere que la gestión de incidentes para este componente se brinde en modalidad 24x7.
13.12	Se requiere que la gestión del cambio para este componente se brinde en modalidad 8x5.
13.13	CFN B.P. deberá contar con un acceso de lectura a la plataforma, desde donde se podrá visualizar información y estadísticas asociadas a este componente.

8.1. SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO PREVENTIVO

El servicio de mantenimiento preventivo deberá contener las siguientes características:

- Ser provisto directamente por el personal técnico del contratista.
- Realizar una visita técnica anual en cada localidad de acuerdo con el cronograma elaborado de mutuo acuerdo con administrador del contrato designado por la contratante.

Las actividades del mantenimiento preventivo a realizarse como mínimo son:

- Respaldo de configuraciones,
- Revisión de logs de funcionamiento,
- Revisión física del funcionamiento de los componentes, ajustes y calibración de los equipos y software, entre otros,
- Limpieza externa de los equipos,
- Revisión física del funcionamiento de los componentes,
- Ajustes y calibración de los equipos y software,
- Revisión y etiquetado de cables de conexión,
- Pruebas de operación de toda la plataforma, es decir, cada uno de los equipos,
- Revisión de la alta disponibilidad y pruebas de contingencia

Como productos entregables para validar el cumplimiento de las actividades, el contratista deberá entregar a la CFN B.P., el original del informe técnico con el detalle de las actividades realizadas en cada localidad de la CFN B.P. con sus respectivas conclusiones y recomendaciones, así mismo contar con las firmas de responsabilidad del contratista. Deberá ser entregado al administrador del contrato, máximo en 8 días calendario contados desde la fecha del mantenimiento.

8.2. SERVICIO DE SOPORTE TÉCNICO Y MANTENIMIENTO CORRECTIVO

El servicio de soporte técnico y mantenimiento correctivo deberá contener las siguientes características:

Deberá incluir la solución a problemas físicos y lógicos, los cuales incluyen problemas con las configuraciones, problemas de funcionamiento, problemas asociados al diseño, problemas asociados a bugs reportados por el fabricante, asesoría para optimización de configuraciones, realizar tunning y afinamiento de los equipos, los cuales incluyen problemas con las configuraciones, problemas de funcionamiento, problemas asociados al diseño, entre otros.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

El servicio de soporte técnico se realizará las veces que se lo requiera, de acuerdo con incidentes detectados ya sea por el contratista o por la CFN B.P.

El servicio de mantenimiento correctivo incluye la provisión partes y piezas que sean necesarios para el correcto funcionamiento de los equipos y de ser el caso el reemplazo total del equipo (sin costo adicional para la CFN B.P.), cuando el daño sea de tal magnitud que el problema no pueda ser superado con el reemplazo de algún componente. El tiempo de reposición de partes o piezas o equipos será de máximo el siguiente día calendario.

En caso de que un equipo deba ser trasladado por el Contratista a los talleres, para su reparación o chequeo, éste deberá instalar un equipo de similares características y dará el soporte que permita que el servicio quede funcionando, hasta que el equipo sea remplazado o reparado.

El contratista debe proveer la mano de obra especializada para realizar la instalación de versiones y parches, en caso de que se presenten daños durante el periodo de vigencia del servicio.

El servicio de mantenimiento correctivo deberá garantizar la operatividad de la solución de acuerdo al SLA solicitado y en modalidad 24x7x365.

Como productos entregables para validar el cumplimiento de las actividades deberá entregar a la CFN B.P. luego de cada mantenimiento el original del informe técnico en el cual se detalle el tipo de problema y la forma de solución, con sus respectivas conclusiones y recomendaciones, así como las firmas de responsabilidad. Los mismos que deberán ser entregados al administrador del contrato en máximo 8 días calendario contados desde la fecha del mantenimiento.

8.3. SERVICIO DE SOPORTE TÉCNICO Y ACTUALIZACIONES

El servicio de actualización deberá contener las siguientes características:

Comprende que toda la plataforma de Seguridad Perimetral Gerenciada a lo largo del plazo del contrato deberá estar en una versión homologada y estable recomendada por el Centro de Operaciones de Seguridad SOC para proporcionar de manera eficiente los servicios solicitados por la CFN B.P.

Las actualizaciones incluyen el despliegue para microcódigos, firmware, software y para todos los componentes de la plataforma.

El contratista será el responsable de tener los equipos en la versión estable y de darse una actualización deberá solicitar una ventana de mantenimiento al contratista adjuntando el plan de actualizaciones.

8.4. SERVICIOS DE INSTALACIÓN Y CONFIGURACIÓN

La prestación del Servicio de Seguridad Gerenciada incluye la provisión del hardware y software necesario por parte del proveedor para proporcionar de manera eficiente los servicios requeridos. El equipamiento por instalarse deberá ser escalable, es decir, permitir la adición y ampliación de los servicios de la plataforma de seguridad gerenciada.

Los sitios en los cuales se debe instalar los equipos para habilitar los servicios requeridos por la CFN B.P. se detallan en Tabla 1: Localidades de CFN para el despliegue del servicio debe cumplir con los siguientes requerimientos:

- La instalación de toda la solución requerida deberá ser realizada por el contratista, a su costo y bajo su responsabilidad.
- El tiempo para la instalación y configuración de los equipos para habilitar los servicios será de 15

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

días calendarios contados a partir de la suscripción del contrato.

- El contratista deberá realizar las configuraciones de todos los equipos que necesite instalar para la provisión de servicios, de acuerdo con las necesidades definidas por la CFN B.P. Los parámetros básicos son: configuraciones de las interfaces, nombres de host, accesos de gestión, usuarios y privilegios de todo el equipamiento ofertado, esquema de direccionamiento IP, nomenclaturas y políticas definidas en el documento de ingeniería de detalle y la metodología de proyectos aprobado por la CFN B.P.
- La CFN B.P., proveerá el espacio con condiciones físicas, ambientales, de energía en los centros de Datos de Quito y Guayaquil.
- El servicio de instalación comprende el ensamblaje e instalación física de los equipos en los racks, instalación de máquinas virtuales de requerirse, conectorización de los patchcords UTP apantallados y realizar el etiquetado de equipos y patchcords, para lo cual la CFN B.P. proveerá las facilidades de acceso a sus centros de cómputo.
- .El contratista deberá portar todos los instrumentos y herramientas necesarias para la correcta instalación y pruebas de operación del equipamiento ofertado para la adecuada prestación de los servicios solicitados.
- El contratista será responsable de la instalación física, energizar e interconectar las interfaces de todo el equipamiento requerido para la provisión de los servicios.
- Luego de la implementación de todos los servicios se deberá entregar el documento acorde a la metodología de proyecto de la CFN Arquitectura Definitiva que contenga lo siguiente:
  - ✓ Configuraciones implementadas (detalle minucioso)
  - ✓ Capturas de pantalla.
  - ✓ Acogerse a la metodología de proyectos de la CFN B.P. para los entregables

  El documento puede ser entregado en medio digital y será recibido por el Administrador del contrato en máximo 5 días laborales posteriores a la implementación

8.5. OTROS SERVICIOS ESPECIALIZADOS

8.5.1. Servicios de Contingencias

Con el fin de garantizar la continuidad del negocio de la CFN B.P., el contratista debe configurar en sus equipos, la Alta Disponibilidad (HA) para que en caso de que el centro de datos principal en la ciudad de Quito quede fuera de operación, los equipos del centro de datos alterno en la ciudad de Guayaquil asuman todo el procesamiento de solicitudes y perfilamientos y servicios a nivel nacional.

Por lo tanto, debe considerarse un despliegue distribuido de la solución para la CFN B.P., con un clúster comprendido entre ambas localidades y tener un esquema de Alta Disponibilidad, para poder ejecutar el plan de contingencia y de recuperación de desastres de la CFN B.P. que involucra a las oficinas sucursales inclusive, sin inconvenientes, para lo cual, se debe considerar que las oficinas sucursales deberán ser controladas remotamente distribuyendo la carga hacia cada concentrador de acuerdo a la siguiente distribución:

Región 1: Latacunga, Ambato, Riobamba, Esmeraldas e Ibarra su concentrador principal es Quito.

Región 2: Cuenca, Loja, Manta, Machala, su concentrador principal es Guayaquil.

La solución de Seguridad perimetral Gerenciada deberá integrarse a la base de datos del directorio activo que existe en el centro de datos Quito y en el centro de datos Guayaquil de la CFN B.P.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

El contratista deberá instalar todas las funcionalidades que se ha solicitado y será responsabilidad del contratista que cuente con todas las licencias para activar los módulos solicitados para brindar el servicio según lo especificado por la CFN B.P en el tiempo indicado.

8.5.2. Servicios de Monitoreo Proactivo

El contratista deberá contar con un centro de monitoreo y gestión especializado, diferente al Centro de Atención de Clientes.

El contratista deberá contar con la atención centro de monitoreo y gestión especializado con una modalidad de atención 24x7x365.

El contratista deberá comprometerse a tener una metodología de trabajo bajo la cual se realice la ejecución de las tareas operativas y la continua gestión y administración de la plataforma de Seguridad Gerenciada, que se basen en las Mejores Prácticas y Recomendaciones ITIL, metodología de trabajo presentada en su oferta y mantener concordancia con las buenas practicas descritas en la ISO270001 para la detección oportuna de prevención de incidentes de seguridad.

El contratista deberá contar con personal técnico dedicado para el envío y análisis de los informes mensuales del desempeño de la plataforma de Seguridad Gerenciada y mostrar el cumplimiento del Acuerdo de Nivel de Servicios (SLA); este rol deberá ser coordinado por el supervisor del contrato y deberá acordar mensualmente con el administrador del contrato de CFN la revisión de los informes presentados y las definiciones de mejoras a satisfacción de la contratante.

El contratista deberá contar con personal técnico dedicado como parte del escalamiento para incidentes de carácter crítico; este rol deberá ser ejecutado por el arquitecto de la solución solicitado en el apartado de Experiencia del personal técnico mínimo.

El contratista deberá facilitar el acceso al Centro de soporte del proveedor (portal web) para visualizar los tickets aperturados por la contratante y dar seguimiento a las peticiones sean cambios o incidentes de la plataforma de Seguridad Gerenciada, así también deberá darse acceso de lectura a los portales de las herramientas necesarias para visualizar el desempeño como mínimo del WAF, NGF, AVAS, SSL VPN de la solución implementada. La entrega de las credenciales al administrador del contrato de CFN deberá remitirse mediante oficio máximo a los 15 días posteriores de la firma del contrato, durante la fase de implementación y pruebas de todos los servicios contratados.

La recolección de datos de CFN deberá estar soportada en una base de datos o repositorio del proveedor; se almacenará información de hasta un año de antigüedad.

9. ENTREGABLES

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

Entregable	Plazo
Certificado del portal del fabricante indicando que se posee el licenciamiento para el tiempo del contrato	15 días calendario posteriores a la firma del contrato
Documento de Arquitectura Definitiva o Memoria Técnica de la solución implementada	Deberá entregarse 5 días después de culminada la implementación
Informe de Mantenimiento Correctivo	Máximo 5 días laborables posteriores a la

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

	realización de este.
Informe de Mantenimiento Preventivo	Máximo 5 días laborables posteriores a la realización de este
Informe sobre deficiencias del servicio	Máximo de 72 horas laborables
Certificados de Transferencia de Conocimientos	3 días laborables posteriores a la transferencia de conocimientos que deberá ejecutarse dentro del primer trimestre
Tabla de costos de los servicios	A la suscripción del contrato
Cronograma de mantenimiento preventivo	15 días calendario posteriores a la firma del contrato
Informe técnico mensual (de disponibilidad) de prestación del servicio	Dentro de los primeros 7 días laborables de cada mes Se deberá especificar el cumplimiento del Acuerdo de Nivel Servicio (SLA)
Factura correspondiente al mes del servicio brindado	Dentro de los primeros 10 días laborables de cada mes En caso de no cumplirse con este requerimiento el pago se cancelará en el mes subsiguiente.

Nota: Para la atención de inconsistencias en entregables, una vez comunicada la inconsistencia por parte de la CFN B.P., el contratista tiene máximo 3 días laborables para entregar los documentos corregidos sean estos: facturas, informes de disponibilidad o actas de servicios.

10. PLAZO TOTAL DE LA CONTRATACIÓN

El plazo total para la ejecución del contrato será de 730 días calendarios, contados a partir de la suscripción del contrato, considerando que dentro de los primeros 15 días se realizará la actualización de licencias y afinaciones en la plataforma.

Posterior a los 15 días de actualización de licencias y afinaciones en la platafoma, se suscribirá entre el supervisor designado por la contratista y el administrador del contrato de CFN B.P. un acta entrega recepción parcial de todos los servicios funcionales a satisfacción de la CFN B.P.

11. FORMA DE PAGO

La CFN B.P. pagará los valores por concepto de prestación de servicios de forma mensual, contra entrega de los siguientes documentos:

- Informe técnico de disponibilidad
- Informe de conformidad del Administrador del Contrato
- Emisión de la factura correspondiente

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Para el último pago de los servicios recibidos, deberá también suscribirse como parte de los documentos entregables el acta entrega recepción definitiva acorde a lo dispuesto en el artículo 124 del reglamento a la LOSNCP.

NOTA: Los valores a cancelar por los servicios recibidos mensualmente se regirán al cumplimiento de los SLA's correspondientes.

12. OBLIGACIONES DEL CONTRATANTE

Además de las obligaciones establecidas en los presente términos de referencia, la CFN B.P. se compromete en:

- Brindar las facilidades y accesos correspondientes para que el personal técnico de la contratista realice las actividades de soporte técnico y mantenimiento correctivo, mantenimiento preventivo, actualización y transferencia de conocimientos.
- Cumplir con las obligaciones establecidas en el contrato, y en los documentos del mismo, en forma ágil y oportuna.
- Delegar un administrador de contrato, el mismo que será el único canal que tomará contacto con el contratista
- Entregar en un plazo de 15 días posteriores a la suscripción del contrato el detalle de la Metodología de Proyectos de la Gerencia de Tecnologías de la Información de la CFN B.P. al proveedor.

13. OBLIGACIONES DEL CONTRATISTA

Además de las obligaciones establecidas en los presente términos de referencia, la CFN B.P. se compromete en:

- Brindar el Soporte de mantenimiento preventivo y correctivo; y, actualización de la plataforma de Seguridad Perimetral Gerenciada de acuerdo con el SLA solicitado mismo que incluye lo siguiente:
- Habilitar el acceso a soporte Técnico y Actualizaciones de Firmware, Software y Parches por el tiempo de vigencia del contrato.
- Brindar el servicio de Mantenimiento Preventivo del software empleado en la plataforma de Seguridad Gerenciada por el tiempo de vigencia del contrato.
- Brindar el servicio de soporte técnico especializado para todos los servicios solicitados por la CFN B.P. que tendrán una modalidad de atención 24x7x365.

14. GARANTÍAS

El oferente adjudicado deberá entregar una Garantía Técnica de acuerdo con el anexo correspondiente, en la que se avale el buen funcionamiento y disponibilidad del servicio; así como el cumplimiento de de todos los servicios solicitados, mantenimientos preventivos y correctivos, actualizaciones de firmware, soporte técnico para los componentes de la plataforma de Seguridad Gerenciada, en base a los términos detallados en el presente documento durante 730 días calendarios, contados desde la firma de la firma del contrato.

Para la garantía técnica, la CFN B.P. no asumirá costo adicional para las actualizaciones de Software, Firmware, Parches de Seguridad, cambio de partes piezas, accesorios o mano de obras; estos costos deben ser asumidos por el contratista. La garantía técnica y soporte en modo 24x7x4 deber ser brindado por el oferente para el reemplazo de partes y piezas.

15. MULTAS

Las multas deberán aplicarse de la siguiente forma:

Por falta de implementación y puesta en funcionamiento de los servicios, el oferente, cancelará una multa del 1x1000 por cada día de retraso, del valor proporcional de los servicios que no se encuentren implementados o funcionando, 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 cinco (5) días subsiguientes de ocurridos los hechos. Una vez transcurrido este plazo, de

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

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.

Los costos asociados al incumplimiento de la disponibilidad de cada uno de los servicios se calcularán de acuerdo a la siguiente tabla:
Los niveles de disponibilidad se aplicarán de manera independiente para cada equipo
Para efectos de penalización se considerará el valor de cada uno.

DISPONIBILIDAD PARA 99.8%

% de Disponibilidad mensual		Tiempo fuera de servicio		Valor mensual
Desde	Hasta	Desde	Hasta	
100,00	99,80	0,00 h	1,44 h	0%
99,79	99,30	1,43 h	5,04 h	10%
99,29	93,00	5,03 h	3,60 h	20%
92,99	75,00	3,59 h	50,40 h	30%
74,99	0,00	50,30 h	180,00 h	50%

Nota: Tabla calculada al 99.8% de disponibilidad tomado como referencia un mes de 30 días

DISPONIBILIDAD PARA 99.9%

% de Disponibilidad mensual		Horas mensuales fuera de servicio		Valor mensual
Desde	Hasta	Desde	Hasta	
100,00	99,90	0,00 h	0,72 h	0%
99,89	99,50	0,71 h	3,60 h	10%
99,49	95,00	3,59 h	36,00 h	20%
94,99	75,00	35,99 h	180,00 h	30%
74,99	0,00	179,99 h	-	50%

Nota: Tabla calculada al 99.9% de disponibilidad tomado como referencia un mes de 30 días

Créditos por SLA Tiempo de Atención de Solicitudes de Cambio:

Exceso de horas por sobre SLA	Porcentaje de Crédito sobre el costo del Servicio Afectado
Más de 2 horas	5%
Por cada hora adicional	0,5%

Créditos por SLA Tiempo de Respuesta de Incidentes:

DESDE (*)	HASTA (inclusive) (*)	Porcentaje de Crédito sobre el costo del Servicio Afectado
0	3	5%
3	5	10%
5	10	15%
10	En adelante	20%

(*) Horas promedio en exceso.

De existir incumplimientos en la atención por parte del contratista a los siguientes requerimientos, se aplicará una multa del 0.5 por ciento (0.5/100) del monto del servicio mensual facturado por cada día de retraso.

- Plazo detallado en la sección Entregables
- Atención de inconsistencias de facturas o informe de disponibilidad del servicio. Comunicadas la inconsistencia por parte de la CFN B.P el contratista tiene máximo 3 días laborables para entregar los documentos consensuados sean estos: facturas, informes de disponibilidad o actas de servicios.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

- En el caso de que la CFN B.P. requiera de un informe sobre la deficiencia del servicio se deberá entregar en un máximo de 72 horas laborables.
- El acuerdo de confidencialidad

El 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.

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 proveedor.

16. LOCALIDAD

El Servicio de Seguridad Gerenciada de la CFN B.P. se ejecutará en las ciudades de Guayaquil y Quito; sin embargo, se recalca que soporta los servicios a nivel nacional.

Elaborado por:	Revisado/Aprobado por:
Ing. Andrea Rodríguez F. **Ingeniero de Servidores y Sistemas Operativos 2**	Ing. José Játiva U. **Gerente de Tecnologías de la Información**

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

ANEXO 1
ACUERDO DE NIVEL DE SERVICIO

Yo, ..., en mi calidad de REPRESENTANTE LEGAL de ....., con RUC ....., de conformidad con lo establecido en la NORMATIVA DE LA SUPERINTENDENCIA DE BANCOS, 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 GESTION DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral 14, literal b, i: "*Niveles mínimos de calidad del servicio acordado*", me comprometo a brindar el servicio contratado en relación al proceso de **CONTRATACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL,** conforme a:

Mecanismos activos de protección	**Nivel de disponibilidad Solicitado (%)**
Cortafuegos (Firewall) de siguiente generación en un esquema de Alta Disponibilidad (HA) en modo Activo /Pasivo, tanto en Quito como en Guayaquil.	99,80%
Balanceo de carga de enlaces para tráfico saliente	99,80%
Acceso VPN IPSEC, VPN SSL	99,80%
Filtrado de navegación Web con inspección de contenido SSL	99,80%
Control de Aplicación con mecanismos y firmas para Anti-Bot	99,80%
Protección contra Intrusos (IPS)	99,80%
Antivirus Perimetral	99,80%
Antivirus y Antispam para correo electrónico	99,90%
Web Application Firewall con protección de contra ataques distribuidos de denegación de servicio (DDOS) a nivel de aplicación.	99,90%
Componentes de Control y Administración	**Nivel de disponibilidad Solicitado (%)**
Sistema de Analítica y Manejo avanzado de Reportes	99,80%
Sistemas de Emulación de Incidentes de Seguridad (sandboxing)	99,90%

- Periodo de Evaluación: Mensual.

  Los tiempos de indisponibilidad del servicio serán contabilizados desde el momento de notificación del incidente al Centro de soporte del proveedor

Esquema de atención:

La atención requerida para Cambios e Incidentes que pueden ocurrir durante la prestación del servicio deberá considerar los siguientes requerimientos mínimos.

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

Gestión de Cambios:

Descripción	Respuesta inicial	Tiempo de ejecución
Cambios sobre módulos gestionados por el proveedor: configuraciones de software base (firmware), configuraciones de alta disponibilidad, configuraciones de gestión y configuraciones de red.	4 horas a partir de la notificación en el Centro de soporte del proveedor	Hasta 24 de horas de ejecución contra conformidad de CFN B.P.
Consultas generales que el personal de CFN B.P. requiera sobre la validez de una configuración sobre módulos que contemplen administración compartida.	4 horas a partir de la notificación en el Centro de soporte del proveedor	Hasta 24 de horas de ejecución contra conformidad de CFN B.P.
Asistencia y acompañamiento en cambios sobre todas las funcionalidades del servicio: módulos con gestión compartida y módulos con gestión del proveedor.	4 horas a partir de la notificación en el Centro de soporte del proveedor	Deberá ser dentro de 48 Horas, después de que CFN B.P. lo solicite al centro de soporte del proveedor.

Gestión de Incidentes:

Prioridades de atención y resolución de Incidentes:

- **Prioridad Alta:** Cuando el servicio o equipo se encuentre caído lo cual impacta a la disponibilidad. El tiempo máximo transcurrido desde el reporte del incidente hasta su resolución es de 1 hora. El proveedor deberá mantener informado al contratante cada cuatro (4) horas hasta la estabilización del servicio durante las siguientes 72 horas de reportado el incidente, que será el tiempo máximo para cerrarlo.

- **Prioridad Media:** Cuando se tenga una degradación en el servicio; pero está aún no afecta la disponibilidad del servicio o equipo. El tiempo máximo transcurrido desde el reporte del incidente hasta su resolución es de 2 horas. El proveedor deberá mantener informado al contratante cada ocho (8) horas hasta la estabilización del servicio durante las siguientes 72 horas de reportado el incidente, que será el tiempo máximo para cerrarlo.

- **Prioridad Baja:** Cuando no hay afectación a la disponibilidad del servicio o no hay degradación del servicio, pero se requiere ejecutar un mantenimiento. El tiempo máximo transcurrido desde el reporte del incidente hasta su resolución es de 8 horas. El proveedor deberá mantener informado al contratante cada día hasta la estabilización del servicio durante las siguientes 72 horas de reportado el incidente, que será el tiempo máximo para cerrarlo.

Tiempo de resolución en caso de necesitar cambio de partes o piezas:

- Una vez determinado el diagnóstico del daño por parte del proveedor, el tiempo máximo para solución para el reemplazo de partes o piezas es "Siguiente Día Calendario". Entendiendo que la reparación incluye las siguientes actividades: identificación de la causa, acciones correctivas y el restablecimiento del estado normal de operatividad; es decir, que el problema detectado haya sido resuelto en su totalidad.

Niveles de escalamiento:

- **Primer nivel:** Mediante atención telefónica o correo electrónico; la CFN B.P. realizará el seguimiento respectivo del caso reportado

- **Segundo nivel:** El contratista deberá proporcionar soporte local en sitio; para ello, el contratista deberá contar con técnicos certificados para clarificar, aislar y resolver problemas relacionados con la infraestructura objeto del proceso de contratación

- **Tercer nivel:** Cuando sea requerido, el contratista, escalará el caso al siguiente nivel de soporte en un Centro Internacional de Soporte Técnico del fabricante. El número de caso

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

asignado por el Centro Internacional de Soporte Técnico del fabricante deberá ser proporcionado al cliente para efectos de seguimiento, y será obligación del Contratista mantener informados del estado/progreso en la resolución del caso, a los técnicos del cliente.

Penalizaciones:

- En caso de existir incumplimiento en los tiempos de atención o resolución de incidentes, definidos en el SLA, la contratante descontará de los pagos mensuales los valores que correspondan.
- Los costos asociados al incumplimiento de la disponibilidad de cada uno de los servicios se calcularán de acuerdo a la tabla indicada en la sección de multas.

FIRMA DEL OFERENTE, SU REPRESENTANTE LEGAL, APODERADO O PROCURADOR COMÚN (según el caso)

(LUGAR Y FECHA)

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

CORPORACIÓN FINANCIERA NACIONAL

ANEXO 2
ACUERDO DE TRANSFERENCIA DE CONOCIMIENTOS

Yo, ..., en mi calidad de persona natural / REPRESENTANTE LEGAL de ....., de profesión ....., con número de cédula ....., me comprometo a prestar los servicios acorde a lo señalado 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 14.b.v: Transferencia del conocimiento del servicio contratado y entrega de toda la documentación que soporta el proceso o servicio", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, deberá incluir en su oferta un "ACUERDO DE TRANSFERENCIA DE CONOCIMIENTOS", donde estipule como mínimo lo siguiente:

- Brindar una transferencia de conocimientos basada en la administración de los equipos bajo el esquema solicitado de administración compartida, por lo cual deberá ser interactiva, exponiendo las limitaciones de los permisos asignados al personal de la Gerencia de Tecnología de la Información.
- La transferencia de conocimientos se deberá realizar dentro del primer trimestre contado a partir de la suscripción del contrato.
- La transferencia de conocimientos se la realizará como mínimo a 6 funcionarios de la CFN B.P indicados por el Administrador del contrato, está se brindará en las instalaciones del contratista en la ciudad de Quito, deberá tener un mínimo de 20 horas y debe incluir el material didáctico y físico emitido a los participantes.
- La transferencia de conocimientos debe ser realizada por el personal capacitado y calificado del contratista 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, el Contratista deberá entregar certificados de participación, el mismo que debe contener: tema, número de horas de duración, nombre del instructor con su firma y sello de la empresa contratista y deberá ser entregado, máximo a los 3 días posteriores a la realización de dicha trasferencia.
- La trasferencia de conocimientos no tendrá costo adicional para la CFN B.P.

FIRMA DEL OFERENTE, SU REPRESENTANTE LEGAL, APODERADO O PROCURADOR COMÚN (según el caso)

(LUGAR Y FECHA)

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

CORPORACIÓN FINANCIERA NACIONAL

ANEXO 3
ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN Y DATOS

Yo, ..., en mi calidad de persona natural / REPRESENTANTE LEGAL de ....., de profesión ....., con número de cédula ....., me comprometo a prestar los servicios acorde a lo señalado 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 14.b.vi: La confidencialidad de la información y datos", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, deberá incluir en su oferta un "ACUERDO DE CONFIDENCIALIDAD DE INFORMACIÓN Y DATOS", donde estipule como mínimo lo siguiente:

- Será responsabilidad del 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.
- El contratista será responsable del cumplimiento del acuerdo por parte del personal que empleare para la ejecución del contrato.
- El 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.
- El 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.
- El 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.

FIRMA DEL OFERENTE, SU REPRESENTANTE LEGAL, APODERADO O PROCURADOR COMÚN (según el caso)

(LUGAR Y FECHA)

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

CORPORACIÓN FINANCIERA NACIONAL

ANEXO 4

ACUERDO DE DERECHOS DE PROPIEDAD INTELECTUAL DEL CONOCIMIENTO, PRODUCTOS, DATOS E INFORMACIÓN

Yo, ..., en mi calidad de persona natural / REPRESENTANTE LEGAL de ....., de profesión ....., con número de cédula ....., me comprometo a prestar los servicios acorde a lo señalado 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 14.b.vii: Derechos de propiedad intelectual del conocimiento, productos, datos e información, cuando aplique" de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, deberá incluir en su oferta un "ACUERDO DE PROPIEDAD INTELECTUAL" donde estipule 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.

FIRMA DEL OFERENTE, SU REPRESENTANTE LEGAL, APODERADO O PROCURADOR COMÚN (según el caso)

(LUGAR Y FECHA)

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

CORPORACIÓN FINANCIERA NACIONAL

ANEXO 5
ACUERDO DE EQUIPO DE TRABAJO Y SUPERVISOR DEL CONTRATO

Yo, ..., en mi calidad de persona natural / REPRESENTANTE LEGAL de ....., de profesión ....., con número de cédula ....., me comprometo a prestar los servicios acorde a lo señalado 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 14.b.viii: "Definición del equipo de contraparte y supervisor del contrato tanto de la institución del sistema financiero como del proveedor", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, deberá incluir en su oferta un "ACUERDO DEL EQUIPO DE TRABAJO Y SUPERVISOR DEL CONTRATO" donde estipule como mínimo lo siguiente:

..... (*indicar el nombre de la empresa*) cuenta con el siguiente personal técnico:

Supervisor de contrato (1)
Nombre completo:
Número de cédula de identidad:
Lugar de residencia:

Arquitecto de solución (1)
Nombre completo:
Número de cédula de identidad:
Lugar de residencia:

Ingeniero especializado en seguridad (2)
Nombre completo:
Número de cédula de identidad:
Lugar de residencia:

FIRMA DEL OFERENTE, SU REPRESENTANTE LEGAL, APODERADO O PROCURADOR COMÚN (según el caso)

(LUGAR Y FECHA)

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec

ANEXO 6
GARANTÍA TÉCNICA

Yo, ..., en mi calidad de REPRESENTANTE LEGAL de ....., con RUC..... , en relación al proceso de contratación para la **"CONTRATACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL"**, constituyo a favor de la Corporación Financiera Nacional B.P. la presente GARANTÍA TÉCNICA sobre la renovación que se contemplan dentro de los términos de referencia, por lo que declaro bajo juramento y en pleno conocimiento de las consecuencias legales que conllevan faltar a la verdad, que:

En mi calidad de Contratista certifico que el servicio correspondiente a la **"CONTRATACIÓN DEL SERVICIO DE SEGURIDAD PERIMETRAL GERENCIADA DE LA CFN B.P. A NIVEL NACIONAL"**, cumple con los requisitos exigidos por la Corporación Financiera Nacional B.P., en su calidad de Contratante.

GARANTÍA
La garantía ofrecida incluye:

- El buen funcionamiento y disponibilidad del servicio de la Herramienta de antivirus y cifrado de información.
- El cumplimiento de todos los servicios de mantenimiento preventivo, mantenimiento correctivo, actualizaciones y soporte (Técnico y operativo) para la Herramienta de antivirus y cifrado de información.
- Actualización de las versiones de Software, Firmware, Parches de Seguridad o soporte, durante la vigencia del servicio.
- Los gastos de transportación derivados del cumplimiento de la presente garantía para la atención de incidentes y/o servicios reportados previamente.
- Asistencia técnica de conformidad con el acuerdo de nivel de servicios.
- Asistencia operativa de conformidad con el acuerdo de nivel de servicios.

COBERTURA
Esta garantía tendrá una cobertura de:

- 2 años y tendrá concordancia con la vigencia del contrato suscrito entre las partes

VIGENCIA DE LA GARANTÍA

- La GARANTÍA TÉCNICA, entrará en vigencia desde el XX de XXXX de 20XX hasta el XX de XXXX de 20XX.

Particular que se pone en conocimiento para los fines pertinentes.

FIRMA DEL PROVEEDOR, SU REPRESENTANTE LEGAL, APODERADO O PROCURADOR COMÚN (según el caso)

(LUGAR Y FECHA)

Matriz Guayaquil: Av. 9 de Octubre #200 y Pichincha, Centro Financiero Público.
Oficina Principal Quito: Edificio Platinum G, Calle Iñaquito entre Corea y Av. Naciones Unidas, Torre A.
Oficinas: Ambato / Cuenca / Esmeraldas / Ibarra / Latacunga / Loja / Machala / Manta / Riobamba / Salinas.
www.cfn.fin.ec