CORPORACIÓN FINANCIERA NACIONAL

CORPORACIÓN FINANCIERA NACIONAL B.P.

TÉRMINOS DE REFERENCIA PARA LA RENOVACION DE LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS

Noviembre, 2019

Contenido

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

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE RENOVACIÓN DE LAS LICENCIAS DE ANTIVIRUS Y CIFRADO DE ARCHIVOS POR DOS AÑOS

1. ANTECEDES Y JUSTIFICACIÓN

La Corporación Financiera Nacional B.P., es una institución financiera pública, cuya misión es 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, servicios que se ofrecen a la ciudadanía a través de herramientas tecnológicas y sus aplicativos informáticos, ya sean contratadas o desarrolladas por CFN.

Dentro de estas herramientas tecnológicas, está la Suite de Seguridad ESET Endpoint Protection Advanced, instalada en servidores y en los equipos de usuario final la cual nos permite mantener la seguridad y la protección contra ataques de virus informáticos y en la protección de la información de usuario final mediante cifrado, razones por las cuales la institución debe contar con soporte, mantenimiento y el derecho de actualización a las nuevas versiones de esta herramienta y por ende explotar las ventajas que tienen los módulos de la misma (antivirus y cifrado).

Antecedentes de la Contratación

Con este producto la institución ha trabajado desde el año 2013, haciendo renovaciones periódicas del licenciamiento, las cuales se indican a continuación.

Inicio Renovación	Fin Renovación	Tiempo de contrato
24-dic-13	23-dic-15	2 años
24-dic-15	23-dic-17	2 años
01-oct-18	30-sep-19	1 año

La última renovación de la Suite de Seguridad ESET Endpoint Protection Advanced, se realizó el 01 de octubre de 2018, mediante contrato No. 023-2018 con la compañía ITSEGUINFO CIA.LTDA., cuya vigencia fue hasta el 30 de septiembre de 2019.

La Suite de Seguridad ESET Endpoint Protection Advanced ha mantenido a los equipos de usuario final y servidores de misión crítica institucionales, protegidos contra los ataques informáticos del exterior, así mismo ha permitido la protección contra virus informáticos desde la red interna, protegiendo el equipamiento contra infecciones mediante dispositivos de almacenamiento, correos electrónicos o acceso a páginas web no autorizadas, por lo que esta herramienta dispone de todas las funcionalidades que se requiere para proteger los sistemas, así también cuenta con el soporte técnico de los canales autorizados en el país para que en caso de ser necesario, brinde su contingencia con la revisión oportuna de los casos reportados.

El número de licencias a renovar, corresponde a la cantidad de usuarios que laboran en la institución, más los servidores de misión crítica ubicados en los centros de cómputo de Quito y Guayaquil.

Las licencias de la Suite de Seguridad ESET Endpoint Protection Advanced, se encuentran distribuidas de la siguiente manera:

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

Ubicación	Cantidad de licencias Utilizadas de Antivirus	Cantidad de licencias Utilizadas de Deslock
Servidores	180	0
Quito	295	295
Latacunga	1	1
Ambato	12	12
Riobamba	15	15
Ibarra	23	23
Esmeraldas	18	18
Guayaquil	475	475
Manta	36	36
Machala	30	30
Loja	23	23
Cuenca	20	20
TOTAL	1128	948

Base Legal

La CFN B.P. al ser una entidad financiera es regida por la normativa de la Superintendencia de Bancos (SB), que en su LIBRO I.-NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, en el TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, en el CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VII.- SEGURIDAD DE LA INFORMACIÓN estipula:

ARTÍCULO 22.- Las entidades deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente:

n. Aplicar técnicas de encriptación sobre la información crítica, confidencial o sensible;

i. Controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software malicioso;

Así también, en el "LIBRO I: NORMATIVA SOBRE OPERACIONES, TITULO IV: ADMINISTRACIÓN DE RIESGOS, SUBTITULO V: SEGURIDAD DE INFORMACIÓN, CAPÍTULO I: MANUAL DE SEGURIDAD DE LA INFORMACIÓN, de la normativa de la CFN se indica:

SECCIÓN I: POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, literal D. POLÍTICAS GENERALES, Sección: Seguridad del equipamiento y documentación, d) El equipamiento será provisto de mantenimiento adecuado para asegurar que su disponibilidad e integridad sean permanentes.

SECCIÓN II: NORMAS Y ESTÁNDARES DEL CONTROL DE ACCESOS, literal D. NORMAS PARA EL CONTROL DE ACCESOS, numeral 4 Control de Accesos a la Red y Sistemas Operativos, i) El Departamento Nacional de Seguridad Informática y la Gerencia de División de Informática podrán usar los programas necesarios para proteger a la Corporación contra software malicioso, como antivirus, anti-

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

spyware, antiphishing y otros. j) Es responsabilidad de la Gerencia de División de Informática mantener actualizado y estandarizado las herramientas y utilitarios informáticos, incluyendo el antivirus.

SECCIÓN VI. NORMAS Y ESTÁNDARES DE LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN, Literal D. Normas de la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información numeral 7. Política de Fuga de Información, indica en su literal c, La Gerencia de División de Informática deberá garantizar la confidencialidad de la información considerada como sensible que reside en los discos duros de las estaciones de trabajo; así como de la totalidad de la información contenida en los discos duros de los equipos portátiles asignados a los funcionarios de la CFN aplicando técnicas de cifrado de datos, para lo cual se deberá establecer el procedimiento que defina los aspectos técnicos para este fin.

Situación Actual:

Para cumplir lo dispuesto en las "Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos" y en la "Normativa de la CFN B.P." y, considerando que los equipos de computación y servidores de misión crítica deben continuar protegidos contra el ataque de virus informáticos y la información institucional debe estar salvaguardada de accesos no autorizados, robo o fuga de datos, es necesario la renovación de mil ciento veinte y ocho (1128) licencias del módulo de antivirus, y novecientas cuarenta y ocho (948) licencias del módulo de cifrado de información, con los que cuenta la institución, por el período de dos años.

Es importante indicar que de no contar con este servicio se afectaría a la continuidad del negocio, ya que la información institucional estaría expuesta a los ataques de virus informáticos y accesos no autorizados.

Como una solución de seguridad adicional se está solicitando Eset Enterprise Inspector (EDR), el mismo que es parte de la Suite de Seguridad ESET Endpoint Protection Advanced, siendo una solución complementaria, que trabaja en distintas capas de seguridad y en distintas instancias de un posible ataque. Mientras una solución antivirus detecta códigos maliciosos, por ejemplo: exploit, trojanos y los muy comunes ransomware, un EDR va a detectar cambios en el sistema que podrían estar dando indicio de un ataque.

2. OBJETO DE LA CONTRATACIÓN

Renovación de las licencias con los que cuenta la institución, por el período de dos años, de acuerdo con el siguiente detalle:

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

3. OBJETIVOS

- Contar con una herramienta de seguridad y protección contra ataques de virus informáticos y otras amenazas de software malicioso (malware).
- Salvaguardar la información institucional de accesos no autorizados, mediante el cifrado de información.

4. ALCANCE

La presente contratación tiene como alcance contar con la renovación de mil ciento veinte y ocho (1128) licencias del módulo de antivirus y novecientas cuarenta y ocho (948) licencias del módulo de cifrado de

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

información de la Suite de Seguridad ESET Endpoint Protection Advanced con los que cuenta la institución, por el período de dos años, para todos los equipos de computación (escritorio y portátiles) y servidores de la CFN B.P., a nivel nacional,, adicionalmente también se va a instalar en las computadoras institucionales, el módulo ESET Enterprise Inspector, que es una solución complementaria de seguridad para detectar cambios en el sistema operativo, que podrían convertirse en ataques de virus informáticos en la red.

5. METOLOGÍA DE TRABAJO Y REQUERIMIENTOS POR GESTIÓN DE RIESGO OPERATIVO

5.1 Metodología de trabajo

La metodología de trabajo, contempla los siguientes aspectos:

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

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

5.1.3 El soporte técnico estará vigente durante la vigencia del contrato y deberá tener las siguientes características mínimas:

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

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:

A. Acuerdo de nivel de servicio (SLA)

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

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

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

i. Tiempos de respuesta y reparación para el servicio

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

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

ii. Prioridad de Servicio de Soporte:

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

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

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

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

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

iv. Prioridad Media: De carácter "Importante".

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

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

v. Prioridad Baja:

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

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

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

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

vi. Nivel de escalamiento para los incidentes:

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

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

- **Tercer nivel**: Cuando sea requerido, el Contratista, escalará el caso al siguiente nivel de soporte es decir al fabricante (ESET), teniendo que proporcionar a la Contratante el número de caso asignado para efectos de seguimiento, y será obligación del contratista mantener informado del estado/progreso en la resolución del caso, a los técnicos de la Contratante.

vii. Tiempo de resolución:

El tiempo máximo para atención y solución, van como se menciona en el numeral ii prioridad del servicio de soporte.

viii. Penalizaciones:

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

B. 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:

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 personal técnico designado por el contratista, deberá brindar la respectiva transferencia de conocimientos donde se exponga la administración, operación, y monitoreo de la solución instalada en CFN B.P.

- La transferencia de conocimientos se la realizará, a los tres meses de iniciada la vigencia del contrato, por una sola vez, a menos que se libere una nueva versión de la herramienta, en cuyo caso se tendrá que realizar una nueva capacitación por cada versión liberada durante la ejecución del contrato, en la fecha y hora que la CFN B.P. lo requiera; estas capacitación no tendrá ningún costo adicional para la Contratante.

- La transferencia de conocimientos se deberá realizar como mínimo a 4 funcionarios de la CFN B.P. en las instalaciones de la CFN B.P. en la ciudad de Quito y deberá tener un mínimo de 2 horas, deberá incluir el material didáctico y físico para los participantes.

- La transferencia de conocimientos debe ser realizada por el personal capacitado y calificado, presentado en la oferta, de manera presencial.

- La transferencia de conocimientos debe ser coordinada por el administrador del contrato.

- Como productos entregables de la fase de transferencia de conocimientos, el Contratista deberá entregar acta de transferencia de conocimientos, certificados de participación, el mismo que debe contener: tema, número de horas de duración, nombre del instructor con su firma y sello de la empresa proveedora y deberá ser entregado, máximo a los 3 días posteriores a la realización de dicha trasferencia.

- La transferencia de conocimientos, no tendrá costo adicional para la CFN B.P.

C. 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:

- 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.

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 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.

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

D) 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.

E) Acuerdo del equipo de trabajo y administrador/supervisor del contrato en el proveedor

De conformidad con lo establecido en el Libro I.- NORMAS DE CONTTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO, TITULO IX.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS, CAPITULO V.- NORMA DE CONTROL PARA LA GESTIÓN DEL RIESGO OPERATIVO, SECCIÓN VI.- SERVICIOS PROVISTOS POR TERCEROS, ARTICULO 14, numeral b., viii: Definición del equipo de contraparte y administrador/supervisor del contrato tanto de la entidad controlada como del proveedor", de la Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos, 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.

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

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

6. INFORMACIÓN QUE DISPONE LA ENTIDAD.

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

- Dos consolas de administración de la Suite de Seguridad ESET para el módulo de antivirus, las mismas que son independientes para Quito y Guayaquil y están divididas para sus regionales (región 1 y región 2).
- Una consola centralizada de administración de la Suite de Seguridad ESET para el módulo de cifrado de información en Quito, a la cual se reportan todos los equipos de cómputo que tienen instalado la licencia de este módulo a nivel nacional.

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

MODULO	**LICENCIAS A RENOVAR**
ANTIVIRUS	1128
CIFRADO	948

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

Licencias		**Cantidad**	**Total**
Cifrado	Estándar	590	948
	Pro	358	

Existe una variación en la cantidad de licencias adquiridas del módulo de cifrado de información, en comparación del contrato anterior, esto se debe a que la institución renovó los equipos de escritorio que se encontraban fuera de vigencia tecnológica y los reemplazo por equipos portátiles, por lo que es necesario aumentar el número de licencias PRO y disminuir la cantidad de licencias estándar.

7. PRODUCTOS O SERVICIOS ESPERADOS

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

7.1 DETALLE DE LOS SERVICIOS REQUERIDOS

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

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

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

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

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

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

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

7.2 CARACTERISTICAS DEL PRODUCTO

Protección a nivel de estaciones de trabajo y servidores.	El producto deberá permitir proteger a los equipos contra código malicioso (malware) tal como: Adware, Backdoor, Badware Alcalinos, Bombas, Bomba fork, Bots, Caballo de Troya, Cookies, Crackers, Cryptovirus, Dialers, Exploit, Hijacker, Hoaxes, Jokes, Keystroke o keyloggers, Leapfrog, Parásito Informático, Pharming, Phishings, Pornware, Rabbit, Riskware, Rootkit, Scumware, Spam, Spyware, Ventanas emergentes/POP-UPS, Virus, Worms (gusanos). Protección contra ataques a la red. Protección proactiva sobre aplicaciones de ofimática (Microsoft, Open office). Ser altamente efectivo y fácil de usar. Ofrecer la capacidad de desplegar y administrar fácilmente los productos en las estaciones de trabajo, de modo que se pueda aplicar la política de seguridad corporativa en forma sencilla sin necesidad de imponer grandes exigencias al personal ni a los recursos del sistema.
Administración Centralizada de la solución.	Soporte para múltiples plataformas, debe funcionar tanto en equipos Windows como Linux, Mac, permitiendo instalarse todos los componentes deseados simultáneamente con el programa de

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

	instalación general o eligiendo los componentes individuales Vista general perfecta de la seguridad de la red. Incluir un sensor detector de equipos no autorizados, descubrir todos los equipos de la red que no están protegidos ni administrados y mostrárselos al administrador. Grupos dinámicos y estáticos, asignar clientes a grupos estáticos o dinámicos y establecer los criterios de inclusión para cada grupo dinámico; los clientes designados deben pasar a pertenecer automáticamente al grupo respectivo. Definir las tareas específicas que se deben ejecutar y en qué momento. Permitir manejar todas las licencias a través de una sola consola de administración, en forma transparente desde un solo lugar. Crear múltiples cuentas de usuarios y personalizarlas, los privilegios para cada una se podrán personalizar en forma individual. Se podrá usar en muchas ubicaciones distintas y permitir definir políticas corporativas para los administradores locales. Utilizar el estándar de Seguridad de la capa de transporte (TLS) 1.0. También emplear certificados propios creados y distribuidos especialmente para firmar en forma digital y para cifrar las comunicaciones entre los componentes individuales de la solución con el objetivo de identificar a los pares. Limpieza de equipos terminales y servidores de código malicioso y programas inseguros no autorizados instalados en los equipos de cómputo. . Además de mostrar los informes a través de la consola basada en la Web, se pueden exportar en formato PDF y guardar en una ubicación predefinida, o enviarse como una notificación por correo electrónico. Protección contra vulnerabilidades: Mejora la detección de las Vulnerabilidades y Exposiciones Comunes (CVE) en los protocolos más utilizados, como SMB, RPC y RDP. Brinda protección contra las vulnerabilidades para las cuales aún no se publicó o desarrolló la revisión necesaria. Protección ante botnets: Protege ante las infiltraciones por malware de tipo botnet, previniendo el envío de spam y evitando que se lleven a cabo ataques de red desde los endpoints. Desinstalación de soluciones de seguridad: la solución deberá ser capaz de desinstalar la solución que se encuentra instalada actualmente. Instalación/ desinstalación de Software de terceros: La consola deberá tener la posibilidad de desinstalar software instalado en los equipos.

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

	Deberá contar con la posibilidad de sincronizarse con el Active Directory. Debe permitir generar grupos de clientes dinámicos (paramétricos) y grupos estáticos. La consola de gestión debe mostrar la lista de servidores y estaciones que tienen el antivirus instalado. Debe ser capaz de instalarse en un entorno de clúster y ante la caída de un servidor levantar el otro automáticamente sin pérdida alguna de datos ni de disponibilidad. Que al ejecutar un análisis en un endpoint el consumo de memoria del servidor sea menor a los 23Mb.
Protección para Plataformas Windows, Linux y Mac OS	El Producto deberá proteger las siguientes plataformas: Sistemas operativos Microsoft Windows XP SP3, con disco de 300 GB, RAM de 512 MB con red. Microsoft Windows Vista SP1 Microsoft Windows 7, Microsoft Windows 8, Windows 10. Versión para servidores: Microsoft Windows Server 2016, 2012R2, 2012, 2008R2, 2008, 2003. Microsoft Windows Server Core 2012R2, 2012, 2008R2, 2008 Core. Microsoft Small Business Server 2011, 2008, 2003R2, 2003. Linux Mac OS
Protección en tiempo real	El producto deberá contar con protección en tiempo real a través de tecnología denominada como Heurística Avanzada, además de su protección reactiva en base a firmas, lo cual permita detectar y detener todo tipo de código o software malicioso alojado en unidades de discos duros fijos o removibles.
Filtrado de correo electrónico	El producto deberá examinar con eficiencia los buzones de entrada de los usuarios finales en busca de spam, ataques de phishing y mensajes de correo electrónico no solicitados. Las listas blanca y negra, así como el aprendizaje automático, se pueden configurar en forma separada para cada cliente o grupo. El soporte nativo para Microsoft Outlook mejora la protección (POP3, IMAP, MAPI, HTTP) ante amenazas en línea sin generarle trabajo adicional.
Filtrado de SPAM en correo electrónico.	El producto deberá ofrecer un módulo antispam que permita realizar análisis en tiempo real.
Filtrado de Navegación	Deberá tener filtrado de navegación realizando la búsqueda en tiempo real de códigos maliciosos en tráfico HTTP y HTTPS, debiendo filtrar el código malicioso antes de que se escriba en las carpetas temporales del disco duro. Ofrecer una alta velocidad de exploración con un mínimo impacto en el sistema, lo que lo ayudará a preservar el rendimiento de los equipos corporativos, a mantenerlos funcionando

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

	sin problemas y a extender la vida y la usabilidad del hardware.
Protección Proactiva	El Producto deberá contar con protección proactiva y reactiva para impedir modificaciones al sistema (cambios en el registro). Proteger la infraestructura crítica corporativa durante el período crucial posterior a los brotes de malware. La tecnología de heurística avanzada deberá proteger los endpoints e impedir que los códigos maliciosos logren abrirse paso en la red.
Tecnología de heurística avanzada	Utilizándola para la detección heurística de malware para proteger los sistemas corporativos de las amenazas conocidas y emergentes, a la vez que mantener los falsos positivos en un mínimo. Que permita la optimización inteligente mediante configuración predefinida, que proporcione la combinación más eficiente de la protección del sistema y la velocidad de la exploración.
Instalación por componentes	La protección de correo electrónico deberá tener la posibilidad de instalarse por componentes, puede elegir los componentes a añadir o eliminar.
Tecnología de Emulación	La solución ofertada deberá contar con una tecnología que someta al código malicioso a una monitorización activa, mientras se ejecuta en un entorno protegido (también conocido como "sandbox"). Basándose en el comportamiento del código, esta tecnología determinará si la muestra dada representa una amenaza e inmediatamente marca o elimina todas las aplicaciones dañinas.
Heurística avanzada en medios extraíbles y ejecución de archivos	Que emule el código en un entorno virtual y evalué su comportamiento antes de que se permita la ejecución del código desde un medio extraíble.
Bloqueo de Exploits	La solución ofertada deberá contar con un sistema de bloqueo de Exploits y debe estar dirigido al problema de vulnerabilidades 0-day (día cero) para las aplicaciones más comunes, como navegadores Web, Java, lectores de PDF y herramientas de Microsoft Office. Debe utilizar una tecnología completamente diferente a las que solo se basan en la detección de archivos maliciosos, y así lograr estar un paso más cerca de los atacantes.
Explorar secuencias de datos alternativas ADS	Que permita la exploración de las secuencias de datos alternativas usadas por el sistema de archivos NTFS, constituyendo asociaciones de archivos y carpetas que son invisibles para las técnicas comunes de exploración.
Tecnología de Análisis de código	La solución ofertada deberá contar con una tecnología de detección al analizar archivos para buscar semejanzas con muestras de códigos maliciosos conocidos antes de que se desarrolle la firma de virus. Basándose en el comportamiento del código, esta tecnología determinará si la muestra dada representa una amenaza e inmediatamente marca o elimina todas las aplicaciones dañinas.
Tamaño del instalador	El tamaño del instalador de la herramienta antivirus, no deberá exceder de 70Mb.
Consumo de recursos de Memoria del Endpoint	Que el producto utilice menos de 120Mb de memoria RAM cuando este inactivo el sistema. Que el producto utilice menos de 250Mb cuando se ejecute un análisis

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

	completo.
Exclusión de archivos del análisis en tiempo real	El producto deberá contar con la opción para realizar exclusiones de archivos del análisis en tiempo real.
Control de acceso web	El producto deberá contar con un control de acceso web, con categorías para definir qué sitios pueden ser accedidos o no dentro de la red. Limitar el acceso a los sitios Web por categoría y por grupo de usuarios para lograr una eficaz aplicación de las políticas corporativas cuyo objetivo es maximizar el cumplimiento de directivas de seguridad y la productividad de los empleados.
Firewall inteligente	Impedir el acceso no autorizado a la red corporativa. Ofrecer una fácil instalación, gran capacidad de personalización de reglas y un modo de aprendizaje inteligente para crear reglas de firewall automáticamente basándose en el tráfico de red observado. Combinar perfiles personalizados de firewall con zonas de redes de confianza.
Análisis manual de búsqueda de códigos maliciosos.	El producto deberá contar con la opción de correr un análisis manual de búsqueda de códigos maliciosos. Ofrecer detección avanzada de malware furtivo mediante la exploración minuciosa del contenido de los protocolos seguros HTTPS y POP3S, así como de los archivos comprimidos.
Control de Dispositivos	El producto debe contar con un control de dispositivos que permita bloquear unidades de CD/DVD, dispositivos de almacenamiento masivo, dispositivos de comunicación USB (incluidos los módems), impresoras USB, Dispositivos Bluetooth, lectores de memorias, entre otros.; además de permitir agregar permisos por usuarios y crear reglas para permitir o denegar el acceso a estos dispositivos. Que los bloqueos a dispositivos puedan realizarse por marca, modelo, número de serie o usuario.
Exclusión de archivos	El producto deberá contar con la opción de realizar exclusiones de archivos del análisis del motor por demanda.
Análisis Programados	El producto y la consola de administración remota deberán permitir realizar análisis programados (bajo demanda) de los discos duros locales de equipos de cómputo. Esta programación se podrá configurar en forma diaria, semanal, mensual.
Cortafuegos de escritorio	El producto deberá contar con un cortafuegos de escritorio (Firewall Personal) que cuenta con un filtrado dinámico de paquetes que provea de monitoreo y filtrado de trafico de Red, y tenga total protección para IPv4 e IPv6 y con la opción de agregar reglas y servicios al cortafuego en forma autónoma y centralizada. Debe poseer distintos modos del módulo de firewall entre los cuales debe tener uno que permita aprender la conducta del usuario generando las reglas permisivas automáticamente. Esta solución no deberá provocar interrupciones con el Firewall Perimetral de la Institución.

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

HIPS (Host-based Intrusion Detection	El producto deberá contar con HIPS (Host-based Intrusion Detection) que proteja su sistema de malware o de cualquier actividad no deseada tratando de afectar negativamente la seguridad de los equipos de cómputo de la CFN B.P. Generar reglas de permiso o denegación sobre aplicaciones cuando estas: depuren otra aplicación, intercepten sucesos desde otra aplicación, intente finalizar o suspender otra aplicación, iniciar una nueva aplicación, o modificar el estado de otra aplicación Generar reglas sobre aplicaciones que intenten realizar las siguientes acciones sobre entradas del registro del sistema: Modificar la configuración del inicio, eliminar entradas del registro, volver a nombrar claves de registro, modificar el registro. Generar reglas sobre archivos que permitan o bloqueen la eliminación, la escritura, el acceso directo al disco, instalar un enlace global o cargar un controlador.
Rollback de base de firmas	El producto antivirus deberá permitir efectuar un Rollback de base de firmas.
Actualizaciones	Que las actualizaciones de base de firmas y componentes ocupen en promedio no más de 0,5Mb diarios y sean programables con intervalos amplios de tiempo.
Actualización a través del servidor de la solución de todas las estaciones protegidas	La consola de administración deberá permitir actualizar a través del servidor de la solución a todas las estaciones protegidas con la posibilidad de tener redundancia de servidores de actualización en forma automáticas (Fail-over).
La actualización de la base de datos de firmas de códigos maliciosos deberá ser incremental, ahorrando de esta manera ancho de banda en su despliegue	Las actualizaciones de las bases de datos de firmas de códigos maliciosos del producto antivirus deberán ser incrementales, evitando de esta manera el ancho de banda en su despliegue.
Opción de apagado luego de escaneo.	La herramienta antivirus debe permitir el apagado luego de la exploración o Repetición de las exploraciones programadas activadas por el usuario. Esto con el objetivo de ayudar a extender la vida útil del hardware y ahorrar energía y optimizar recursos.
Programación y actualizaciones diferidas.	La herramienta antivirus debe contar con una selección opcional para la recepción de actualizaciones provenientes de servidores especiales con 12 horas de retraso para brindar tiempo a los administradores del sistema para evaluar el impacto en su red y asegurar una migración organizada.
Reportes	La consola de administración deberá contar con un mínimo de 36 opciones de reportes gerenciales detallados con información de configuraciones, actualizaciones de los productos, alertas, estadísticas, etc., las cuales pueden ser exportadas a archivos csv y/o html.

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

	Deberá permitir generar reportes gráficos tipo barra, pastel, etc., para una vista rápida de la situación del producto.
Alerta en consola y notificación vía correo electrónico y SNMP	El producto deberá permitir que las acciones de notificación incluyan correo electrónico, SNMP, y entradas de registro.
Compatibilidad con la estructura organizacional del Directorio Activo de servidores Windows para la Instalación del producto	La consola de administración deberá permitir la detección de clientes no registrados sincronizando la estructura del grupo a través de Active Directory.
Análisis de aplicaciones y procesos	Debe permitir clasificar las aplicaciones en al menos 3 grupos según sus características y poder configurar el motor antivirus para que las analice o no. Debe otorgar una puntuación a los procesos en ejecución del sistema para medir su nivel de riesgo.
Análisis de procesos	Deberá poseer una herramienta integrada para ver los procesos en ejecución, los servicios, las conexiones establecidas, claves de registro importantes, programas instalados, actualizaciones de sistema operativo instaladas, logs del equipo, drivers instalados, tareas programadas del sistema, archivo hosts, system.ini y win.ini.
Análisis de archivo comprimidos	El producto ofertado deberá detectar virus en archivos compactados, sin importar el número de niveles de compresión, en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros.
Gestión de Políticas	La consola de administración deberá definir y hacer cumplir consistentemente las políticas a lo largo de la red. El Administrador de Políticas facilitará la importación/exportación, para permitir la aplicación y combinación de las políticas de diversas maneras.
Gestión Multi-plataforma	La consola de administración deberá permitir administrar de forma remota desde una única consola todos los equipos de su red, ejecutando las versiones antivirus en clientes finales y servidores de las diferentes plataformas (Windows, Linux, Mac OS).
Solución para dispositivos móviles (smartphones)	Debe proveer de una solución de seguridad rápida y efectiva para los smartphones corporativos. La herramienta debe tener entre sus características principales las opciones de: Protección contra malware. Función de borrado y bloqueo remoto, Antispam para SMS/MMS., Protección contra desinstalación, Localización de dispositivo por GPS, Auditoría de Seguridad, Bloqueo de llamadas de números desconocidos u ocultos y números no deseados. Que permita definir una lista de contactos permitidos / contactos bloqueados, Cuarentena, Protección contra infiltraciones, Que cuente con administración centralizada, Control de aplicaciones
Seguridad	El producto deberá contener un módulo especial para el análisis de ransomware y amenazas avanzadas así mismo poder realizar informes

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

	sobre cada una de estos eventos de seguridad
Cifrado de datos	Debe proveer de una solución de cifrado simple y potente, usando los algoritmos y estándares más avanzados para crear claves impenetrables: Algoritmos y estándares: • AES 256 bit. • AES 128 bit. • SHA 256 bit. • SHA1 160 bit. • RSA 1024 bit. • Triple DES 112 bit. • Blowfish 128 bit. Certificaciones: • FIPS140-2 level 1.
Administrar las claves de cifrado	Debe tener la capacidad de administrar usuarios y estaciones de trabajo independientemente o en relaciones de "muchos a muchos". Permitir el cambio de las políticas de cifrado en forma remota y silenciosa, sin interacción del usuario.
Tipos de cifrado	Permitir administrar fácilmente cualquier usuario o estación de trabajo en forma remota, incluyendo el uso compartido de claves entre clientes en tiempo real. • Cifrado del disco completo. • Cifrado de medios extraíbles. • Cifrados de archivos y carpetas. • Cifrados de correo. • Cifrado de texto y portapapeles. • Cifrado de discos virtuales y archivos comprimidos.

7.3 - FUNCIONALIDADES TECNICAS EDR Y ANTI APTs

Consola de administración	La solución de EDR debe poder ser instalada On-Premise y administrar con el mismo agente del EPP los equipos finales.
	Permitir tomar acciones desde la consola on premise sobre el equipo final.
	El agente de EDR se deberá poder instalar de manera remota, al menos por

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

	alguno de los siguientes métodos: • Herramienta provista por el propio fabricante. • Línea de comando.
Reportes	La solución de EDR deberá permitir detectar comportamientos sospechosos dentro de los endpoints, en caso de encontrar archivos o procesos extraños, deberá disparar alertas para avisar al administrador.
	La solución de EDR debe proveer un listado de los archivos ejecutables que se ejecutaron dentro de la red.
	La solución de EDR debe proveer un listado de los scripts que se ejecutaron dentro de La red.
	El equipo de seguridad podrá ver qué se vio afectado, dónde y cuándo se realizó el ejecutable, secuencia de comandos o acción específica, y analizar la causa de esto "de vuelta a la raíz".
	Permitir a través de los reportes rastrear los archivos creados en los dispositivos monitoreados, validando su origen, proceso y qué usuario lo creo.
	Los reportes tienen que poder ser editados y ajustados a medida en un archivo excel.
Políticas de seguridad	La solución de EDR deberá permitir la generación de exclusiones utilizando al menos lo siguientes parámetros: • Nombre del archivo • Ubicación del archivo • Equipo • Usuario
	La solución deberá mostrar alertas de seguridad en el equipo del usuario.
	La solución deberá permitir la creación de reglas personalizadas para monitorear determinados comportamientos, por ejemplo: • Modificaciones en llaves del registro del sistema. • Creación de conexiones de red a través de rundll32 • Ejecución de scripts a través de MS Office

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

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

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

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

8. ENTREGABLES

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

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

9. PLAZO TOTAL DE LA CONTRATACIÓN

El plazo para la prestación del servicio será de 733 días contados a partir de la suscripción del contrato, desglosados de la siguiente manera:

- El plazo máximo de tres (3) días calendarios contados a partir de la suscripción del contrato para la entrega del certificado de renovación, en el que certifique la renovación y entrega del licenciamiento de la Suite de Seguridad ESET Endpoint Protection Advanced con las que cuenta la institución.
- El plazo de setecientos treinta (730) días calendario, para la vigencia del licenciamiento de la Suite de Seguridad ESET Endpoint Protection Advanced, que serán contados a partir de la fecha de

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

entrega del certificado de renovación y entrega de las licencias, lo que se indicará en el informe técnico del contratista. Durante la vigencia del licenciamiento y posterior a la entrega del certificado de renovación, el contratista dispondrá un plazo no mayor a veinte (20) días, para realizar la instalación y configuración de las licencias en los equipos de usuario final

10. PERSONAL TÉCNICO / RECURSOS

Para la renovación de licencias de antivirus y cifrado de archivos por dos años, la Institución requiere que se considere como mínimo el siguiente personal técnico:

- 1 Supervisor Técnico
- 1 Ingeniero especializado en la herramienta ESET

11 **FORMA DE PAGO**

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

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

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

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

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

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

Todos los pagos que se hagan a la contratista por cuenta del contrato, se efectuarán con sujeción al precio convenido, a satisfacción de la contratante, previa aprobación del administrador del contrato.

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

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

12 - OBLIGACIONES DEL CONTRATANTE

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

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

11. GARANTÍAS

El contratista deberá entregar al administrador del contrato, dentro de los primeros 3 días hábiles posterior a la firma del contrato, la Garantía Técnica (Ver Anexo 7) del servicio por el tiempo que dure el contrato; garantía que avale el buen funcionamiento y disponibilidad del servicio; en base a los términos detallados en el presente documento, junto con el informe y certificado de renovación de las licencias.

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

12. MULTAS

Las multas deberán aplicarse de la siguiente forma:

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

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

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

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

13. LOCALIDAD

La prestación del servicio será en Quito, en la Av. Iñaquito N36A, entre Naciones Unidas y Corea, Edificio Platinum G

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

Elaborado por:	Revisado/Aprobado por:
JORGE HUMBERTO ORTIZ CARRION Firmado digitalmente por JORGE HUMBERTO ORTIZ CARRION Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000268635, cn=JORGE HUMBERTO ORTIZ CARRION Fecha: 2019.12.04 12:56:04 -05'00' **Ing. Jorge Ortiz** **Ingeniero Soporte a Usuarios 2**	Digitally signed by Jose A. Jativa Ubillus Reason: I am approving this document Location: gye Date: 2019.12.04 13:02:00 -05'00' **Ing. José Játiva U.** **Gerente de Tecnología 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