Términos de Referencia para Solución de Protección de Estaciones y Servidores Contra Malware (v02)

OBJETIVO

El presente documento tiene por objeto establecer la descripción de la o las herramientas que requiere el BNF para la protección de sus estaciones y servidores de computación contra malware como virus, troyanos, spyware, etc.

RESUMEN EJECUTIVO

El BNF necesita contar con una herramienta de protección de estaciones que provea medidas contra diferentes amenazas existentes en el mundo de la informática, las mismas que pueden afectar el desempeño, estabilidad y disponibilidad de los recursos de los sistemas de información en la actualidad y en el futuro. Las características principales son: efectividad contra malware, soporte de actualizaciones frecuentes con un bajo uso de recursos, control centralizado en una consola, implantación a nivel nacional.

ALCANCE DEL PROYECTO

El proyecto incluye la instalación y puesta en producción de un conjunto de herramientas de software y hardware para proveer a los servidores y estaciones de computación del BNF de protección contra malware. Los productos serán instalados en los computadores centrales provistos por el mismo proyecto y en la totalidad de las estaciones que existan en el BNF al momento de la adjudicación. El proyecto de implantación deberá prever todas las condiciones para lograr la instalación exitosa en las estaciones de toda la organización.

El número de equipos donde se implantará la solución es el siguiente:

Tipo de equipo	Cantidad
Estaciones de trabajo (computador personal) ubicadas en las oficinas del BNF a nivel nacional	1800
Servidores de red/aplicaciones/BDD ubicados en la Matriz en Quito, Sucursal Guayaquil y en las 9 oficinas zonales del BNF	60
Cantidad de localidades donde se encuentran las oficinas del BNF a nivel nacional	115

Distribución física de Oficinas

El BNF cuenta al momento con 2 oficinas principales: en Quito (Matriz) y Guayaquil (Sucursal Mayor), a las cuales se conectan directamente el resto de oficinas, es decir, cada sucursal o agencia tiene un enlace de comunicaciones IP con una de las 2 oficinas principales. Se conoce a las oficinas que se conectan a Casa Matriz como Región 1 y al grupo de oficinas que están conectadas a la Sucursal Mayor como Región 2. La topología de la red WAN del BNF determina que haya un servidor

principal de la solución de protección de estaciones y servidores por cada oficina regional, es decir, uno en Quito y uno en Guayaquil. El oferente podrá proponer la ubicación de otros servidores de distribución para optimizar los recursos de comunicaciones en el proceso de actualización de firmas de malware en la red.

Cronograma de Implantación

La empresa que oferte el sistema de protección corporativo deberá instalar y entregar la solución ofertada inmediatamente se firme el contrato de compra. Esta instalación se la realizará en todas las oficinas del BNF según un cronograma planteado por el proveedor y aceptado por el BNF. El oferente debe considerar las condiciones de las oficinas y será su responsabilidad garantizar la instalación exitosa de la herramienta ofertada en cada estación del BNF.
El tiempo previsto para la implantación del proyecto no podrá ser mayor a 90 días a partir de su inicio.

Características de la oferta presentada

El oferente deberá presentar una oferta que incluya al menos:

- Una descripción de la arquitectura de la solución propuesta;
- Una descripción conceptual de la solución;
- La matriz de Bases de cumplimiento de la siguiente sección;
- La documentación de soporte sobre las funcionalidades que cubre la herramienta;
- La descripción de los servicios solicitados;
- La descripción de los otros entregables solicitados.

Bases de cumplimiento para provisión de la Herramienta de protección de estaciones y servidores

La tabla presentada en esta sección describe las funciones y características de los productos y servicios que deberán ofertarse. Cabe notar la presencia de la columna “DESEABLE / MANDATORIO”, que expresa si las características son de cumplimiento obligatorio o no. El cumplimiento de las características deberá ser comprobable con la documentación del fabricante provista por el oferente como parte de la propuesta.

La solución ofertada por las empresas deberá cumplir al menos con los siguientes requerimientos.

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
	Aspectos generales y arquitectura			
1	El oferente deberá presentar en su propuesta una descripción de la arquitectura de la solución incluyendo todos los componentes ofertados: productos y servicios.		M	
2	La propuesta debe incluir una descripción de los servicios complementarios ofertados en la solución.		M	
3	La propuesta debe incluir una descripción de los entregables ofertados según la sección correspondiente de este documento.		M	
4	La herramienta debe proteger estaciones y servidores que funcionen con los siguientes sistemas operativos: Windows 98, Windows XP, Windows 2000 profesional, Windows 2000 server, Windows 2003 server, Windows Vista, Linux Red Hat.		M	
5	La herramienta debe ser una Suite de productos, que cuente con una sola consola de administración central.		M	
6	Los productos componentes de la solución deben ser independientes unos de otros para configuración, control, monitoreo, sin embargo deben ser controlados desde una sola consola de administración.		M	
7	La herramienta de protección de estaciones debe contar con una consola de administración y monitoreo central que controle todos los componentes desplegados (excluyendo la herramienta anti-spam).		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
8	La solución debe incluir la provisión de todas las licencias requeridas que soporten las características solicitadas.		M	
9	La solución debe consistir de la última versión liberada de software disponible a la fecha de adquisición del producto.		M	
10	Incluir medio óptico original con manuales, instaladores, licencias y accesorios correspondientes para el software y hardware propuesto.		M	
11	La propuesta deberá considerar actualización de software de consola, cliente y servidor, Base de datos de firmas de malware, y demás software o información que la herramienta requiera para su normal desempeño por al menos un año.		M	
12	La herramienta deberá incluir su propio mecanismo de actualización de firmas y huellas de malware hacia los servidores de distribución (intermedios) y hacia las estaciones de la red protegidas por la herramienta.		M	
13	El fabricante debe proveer de mecanismos de consulta, soporte, grupos de discusión, boletines, alertas y eventos de seguridad, etc. disponible para el BNF.		M	
14	El fabricante debe registrar al BNF como su cliente para la provisión de los servicios de actualización y notificación que provea directamente.		M	
15	La arquitectura de la solución debe considerar que los servidores principales que eventualmente se ubicarán en Quito y Guayaquil podrán estar configurados en cluster, por lo tanto la herramienta central debe soportar configuración en Cluster de los servidores.		M	Especificar el tipo de configuración de Alta Disponibilidad para los servidores principales

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
	Requisitos para los Servicios Complementarios de la solución			
16	La propuesta debe considerar la desinstalación de otros productos o versiones de software de similares características (protección de estaciones, antivirus, anti-spypware) previamente instalados en las estaciones de trabajo, servidores (como clientes de la solución) y servidores de distribución de la solución.		M	La desinstalación podrá ser provista de forma natural por la herramienta ofertada o usando productos de terceros.
17	La propuesta debe incluir la instalación, implantación y puesta en producción de las herramientas de control central ubicadas en sendos servidores en Quito y Guayaquil.		M	La instalación deberá ser en sitio.
18	La propuesta debe incluir la implantación de la herramienta en el 100% de las estaciones y servidores existentes en el BNF al momento de la contratación.		M	El oferente deberá garantizar que se el producto ofertado quede instalado en todas las estaciones del BNF.
19	La propuesta debe incluir la capacitación para administradores de la herramienta tanto en Quito como en Guayaquil.		M	Los eventos de capacitación para administradores se deberán llevar a cabo en Quito y Guayaquil, para un mínimo de 4 personas por sitio.
20	La propuesta debe incluir la capacitación para el personal de soporte técnico interno del BNF (tanto en Quito como Guayaquil) en tareas de instalación, soporte y solución de problemas en estaciones de usuarios finales.		M	Los eventos de capacitación para personal de soporte se deberán llevar a cabo en Quito y Guayaquil, para un mínimo de 10 personas por sitio.
21	La propuesta debe incluir documentación de soporte sobre las certificaciones de los técnicos de la empresa.		M	
22	Todos los costos de la propuesta deberán estar incluidos. El BNF no incurrirá en desembolsos posteriores por las actividades de implantación.		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
	Requisitos para el funcionamiento de la herramienta			
23	La herramienta debe usar una porción mínima de los recursos disponibles físicamente en las estaciones como memoria, procesador y espacio en disco (especificar cantidad).		M	Especificar la cantidad usada de disco, memoria y procesador.
24	La cantidad de recursos asignados a tareas de verificación de existencia de malware y otras tareas ejecutadas por la herramienta periódicamente en las estaciones debe ser configurable centralizadamente, de forma que el uso de recursos por parte de la herramienta no degrade el desempeño del sistema operativo del computador.		M	
25	La herramienta debe soportar la postergación de las tareas de verificación en caso de afectar el desempeño de las estaciones.		M	
26	El funcionamiento de las verificaciones y actualizaciones debe ser posible de realizar en oficinas remotas cuyos enlaces son de 128Kbps con un promedio de 10 estaciones sin saturar los enlaces de comunicaciones.		M	Especificar el promedio de ancho de banda que utilizaría cada actualización.
27	La herramienta deberá poder instalarse en estaciones con Sistema Operativo Windows XP en español, con al menos 512MB en RAM y procesador Pentium IV o características superiores.		M	
	Consola central de control			
28	La consola debe controlar y monitorear la actividad de los componentes de software de protección de estaciones mediante direcciones IP o nombre de estación de las computadoras personales conectadas a la red.		M	Especificar todos los puertos de comunicación utilizados para este fin.

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
29	La consola central del antivirus debe correr en servidores con Sistema Operativo Windows XP, Server 2000 o Server 2003.		M	
30	La consola debe contar con un cliente de acceso a la misma que permita operar todas sus funciones remotamente. Son aceptables clientes instalados localmente en la estación del administrador o bien características de “web enabled” para tener accesos vía browser de Internet.		M	
31	Las comunicaciones entre las estaciones de trabajo de los usuarios finales y la consola deben usar exclusivamente protocolos UDP o TCP / IP.		M	
32	La consola de administración debe difundir por la red hacia las estaciones administradas, las últimas actualizaciones de los archivos de protección de la base de antivirus y otros componentes de la herramienta.		M	
33	La difusión de archivos o bases de datos de actualización para la protección de estaciones debe hacerse automáticamente mediante calendarización o manualmente a demanda.		M	
34	La consola debe manejar estructura de consolas por jerarquía, es decir, poder manejar una consola maestra y varias consolas esclavas.		D	
35	La consola debe soportar la creación de varios usuarios y grupos de usuarios con configuraciones independientes por grupo o usuario.		D	
36	La consola debe soportar la asignación de perfiles de acceso a cada uno de los usuarios o grupos para administración o acceso a la consola.		D	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
37	La consola debe soportar Servidores intermedios de distribución por grupos de estaciones. Los servidores de distribución pertenecen a diferentes grupos de estaciones. Los servidores de distribución se actualizan desde la consola central y pasan las actualizaciones al resto de equipos dentro de su grupo.		M	
38	La consola central debe soportar multicasting para las tareas de actualización de grupos.		D	
39	En el caso de eventos La consola debe soportar la generación de Alertas en consola y notificación vía correo electrónico, SNMP, SMS u otros servicios de mensajería.		D	
40	La consola deberá ser capaz de generar Reportes gráficos con resúmenes gerenciales de desempeño y resultados de manera automática planificada o a demanda.		M	
41	La consola deberá ser capaz de generar Reportes detallados de desempeño y resultados de manera automática planificada o a demanda.		M	
42	La consola soportará consultas para encontrar equipos con características determinadas como niveles de actualización, nombre de estación, dirección IP, nombre de usuario, etc.		M	
	Funciones de la herramienta de protección de estaciones			
43	La herramienta de protección de estaciones debe contar con por lo menos 200000 firmas y permitirá detectar y eliminar al menos los siguientes tipos de malware en tiempo real: virus, adware, troyanos, spyware, worms, cookies, root-kits, keyloggers, etc.		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
44	Capacidad de detección y eliminación de virus.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
45	Capacidad de detección y eliminación de adware.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
46	Capacidad de detección y eliminación de troyanos.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
47	Capacidad de detección y eliminación de worms.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
48	Capacidad de detección y eliminación de spyware.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
49	Capacidad de detección y eliminación de cookies.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
50	Capacidad de detección y eliminación de rootkits.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
51	Capacidad de detección y eliminación de keyloggers.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
52	La herramienta debe incluir un módulo de Firewall de estaciones.		D	Presentar documentación del fabricante indicando dónde confirmar esta información

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
53	La herramienta debe incluir IDS-IPS para estaciones.		D	Presentar documentación del fabricante indicando dónde confirmar esta información
54	Capacidad de detección y bloqueo de macros maliciosos de MS Office.		M	
55	El firewall de estaciones debe soportar administración centralizada.		M	
56	El firewall u otro componente de la suite debe proveer control de actividad de las aplicaciones.		M	
57	El firewall u otro componente de la suite debe prevenir la modificación no autorizada de archivos del sistema operativo (como el registro de Windows).		M	
58	La tarea de actualización de archivos o bases de datos para la protección de estaciones debe ser sencilla y transparente (no disruptivas) para los usuarios finales de las estaciones.		M	
59	La Instalación y configuración completa del antivirus en los computadores personales de la red podrá realizarse desde la consola de administración central o alternativamente desde una unidad local con acceso remoto a la estación.		D	
60	El antivirus debe manejar opciones de escaneo de archivos de todo tipo de extensiones susceptibles a ser infectados por un virus.		M	
61	El antivirus debe tener la capacidad de detectar y desinfectar los dispositivos de almacenamiento que sean parte de las PCs, como memoria RAM, diskettes, CDs, memorias USB, Discos duros internos, Discos duros externos, etc.		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
62	El antivirus debe detectar en tiempo real las amenazas que existan en dispositivos extraíbles como memorias de estado sólido o discos USB cuando se conectan a la estación.		M	
63	El software de antivirus debe tener la capacidad de poner en cuarentena los archivos infectados.		M	
64	La herramienta de protección debe tener la función de Administrador de archivos en cuarentena		M	
65	La herramienta debe actualizar nuevas firmas de malware identificados por el fabricante vía los servidores de distribución de firmas de malware definidos en la arquitectura de la solución, de manera automática e incremental en cada estación y servidor donde está instalada.		M	
66	El fabricante debe proveer casos documentados de protección de "día cero".		D	
67	La herramienta debe soportar la detección y protección contra virus Polimorfos.		M	
68	La herramienta debe generar un log de registro con la información de las incidencias de amenazas, eventos y análisis.		M	
69	La herramienta debe prevenir la desactivación del software de protección contra malware en estaciones y servidores donde se encuentre activado.		M	
70	La herramienta debe prevenir la desinstalación o borrado del software de protección contra malware en estaciones y servidores donde se encuentre instalado.		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
71	La herramienta debe bloquear el cambio no autorizado de su configuración, impidiendo que los usuarios finales o robots de software puedan desactivar sus funciones.		M	
72	La herramienta debe soportar la desinstalación remota de otras herramientas de seguridad en estaciones remotas.		D	
73	La herramienta debe proveer protección contra virus en archivos del sistema operativo, comprimidos y ocultos.		M	
	Funciones de Protección de datos			
74	La herramienta debe proveer la función de restringir el uso de dispositivos externos y/o extraíbles como: discos externos, CD-ROM, DVD-ROM, discos extraíbles USB, memorias de estado sólido USB, módems, impresoras.		M	
75	La herramienta debe proveer la función de restringir la ejecución de programas alojados en dispositivos externos y/o extraíbles como: discos externos, CD-ROM, DVD-ROM, discos extraíbles USB, memorias de estado sólido USB.		M	
76	La herramienta debe proveer la función de restringir la ejecución de programas particulares en las estaciones.		M	
77	La herramienta debe proveer la administración centralizada de las funciones de esta sección en la misma consola de administración central.		M	
	Los formatos de archivos comprimidos soportados deben ser los siguientes:			
78	7Z		M	
79	ARC		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
80	CPIO		M	
81	GZ		M	
82	JAR		M	
83	RAR		M	
84	TAR		M	
85	TAZ		M	
86	TGZ		M	
87	Z		M	
88	ZIP		M	
89	La herramienta debe soportar la detección y eliminación de amenazas en archivos comprimidos recursivamente.		M	Especificar el número de niveles de soporte para compresión recursiva.
	Protección de Servidor de correo			
90	La herramienta debe proveer un componente de software que instalado en el servidor de correo actual del BNF, MS Exchange 2003, verifique la existencia de virus en el correo entrante o saliente que transita por el servidor.		M	
91	La herramienta debe proveer protección para otros servidores de correo electrónico en la misma modalidad que con Exchange para implantación futura, en especial servidores de Open Source como Zimbra.		D	Especificar qué servidores de correo se soportan
	Protección Anti-spam			
92	La herramienta Anti Spam debe ser una solución de hardware especializado en la función de eliminación de correo spam (appliance).		D	
93	La herramienta anti-spam deberá ser del mismo fabricante que la solución de protección de estaciones		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
94	En caso de ser una herramienta de software, se deberá ofertar el equipo donde la aplicación sería instalada, mismo que deberá cumplir con las especificaciones establecidas para el hardware especializado.		M	
95	La herramienta debe revisar todos los mensajes de correo electrónico dirigidos a los dominios de la Organización que eventualmente serían recibidos en los servidores de correo del BNF.		M	
96	La herramienta debe proveer protección anti-spam para todos los usuarios que tienen protección de antivirus y el resto de componentes de la solución sin afectar el modelo de licenciamiento propuesto.		M	No deberá ser necesario adquirir licencias adicionales de ningún tipo para soportar la protección antispam para todos los usuarios del BNF.
97	La solución anti-spam debe soportar el procesamiento de al menos 500000 mensajes de email entrante por mes sin afectar el rendimiento del servicio de recepción de email.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
98	La solución anti-spam debe soportar el procesamiento de al menos 11 GB de email entrante por mes sin afectar el rendimiento del servicio de recepción de email.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
99	La solución anti-spam debe soportar el procesamiento de al menos 20000 mensajes de email saliente por mes sin afectar el rendimiento del servicio de envío de email.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
100	Los componentes de hardware ofertados deberán ser equipos nuevos de fábrica, no remanufacturados ni usados.		M	Especificar marca, modelo y número de parte de los componentes de hardware ofertados
101	La solución anti-spam debe soportar el procesamiento de al menos 6.5 GB de email saliente por mes sin afectar el rendimiento del servicio de envío de email.		M	Presentar documentación del fabricante indicando dónde confirmar esta información

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
102	La garantía los componentes de hardware deberá ser de 3 años		M	
103	Los equipos de hardware deberán ser 2 equipos en configuración de redundancia y balanceo de carga		M	
104	La herramienta debe eliminar el correo no solicitado con una eficacia superior al 97%.		M	Presentar documentación del fabricante indicando dónde confirmar esta información
105	La herramienta debe tener un mínimo de falsos positivos (menor al 5% de los mensajes marcados como Spam).		M	
106	La herramienta debe permitir la recuperación de mensajes marcados como spam que sean falsos positivos.		M	
107	La herramienta deberá soportar la actualización diaria de firmas anti-spam.		M	
108	La herramienta anti-spam deberá soportar la incorporación de listas locales de criterios de selección de mensajes configurables por el administrador del sistema, como bloqueo de dominios, lista de correos y palabras.		M	
109	La herramienta deberá utilizar adicionalmente análisis dinámicos para detectar spam en tiempo real.		M	
110	La herramienta deberá bloquear el spam en el gateway de mensajería de Internet (el equipo ofertado) y los servidores de correo antes de que se vea afectado el rendimiento de los usuarios.		M	
111	La consola de administración deberá soportar la configuración de las políticas y los niveles de tolerancia frente al spam para grupos o usuarios individuales.		M	

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
112	La herramienta deberá soportar la inclusión de protección contra nuevas amenazas relacionadas con Spam en futuras versiones de software sin necesidad de hacer upgrade de hardware.		M	
113	La inclusión de la herramienta en la red de la Organización deberá acarrear un mínimo impacto (no percibible por los usuarios) en el desempeño del sistema de correo electrónico.		M	
114	La herramienta anti-spam puede presentarse como una solución distribuida en 2 equipos de las características propuestas.		M	
115	La solución debe incluir la implementación de la herramienta anti-spam en modalidad de redundancia de hardware.		M	
116	La herramienta anti-spam redundante debe proveer o soportar mecanismos de balanceo de uso de recursos.		M	
117	La herramienta anti-spam debe proveer la funcionalidad de incluir un mensaje customizado en los mensajes de e-mail salientes.		M	

Descripción de la empresa proveedora

La empresa que provea estos productos y servicios deberá al menos cumplir con los siguientes requisitos.

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
	Características de la empresa proveedora			
1	La empresa proveedora debe ser distribuidora autorizada del producto ofertado y de los servicios de implantación y soporte ofertados.		M	Adjuntar documentación de soporte

Ítem	Requerimiento	Cumple (SI/NO)	Deseable / Mandatario (D / M)	Observaciones
2	La empresa debe tener técnicos certificados que puedan brindar soporte técnico durante el lapso de vigencia del contrato.		M	Adjuntar documentación de soporte
3	La empresa proveedora deberá acreditar la ejecución de proyectos de implantación de la herramienta de protección que está ofertando en un número de estaciones similar o mayor a la del proyecto actual.		M	Adjuntar documentación de soporte
4	La empresa debe proveer soporte técnico por el lapso de duración de las licencia de actualización para eventos relacionados con: instalación del software, configuración, manejo de eventos de afectación masiva.		M	
5	La empresa debe proveer soporte local y externo (dentro y fuera del país) para escalamiento de problemas.		M	
6	La empresa debe proveer una demostración del producto ofertado en el mercado local para evaluar el desempeño de la solución en condiciones similares a las del BNF, tanto de versiones del producto como de tamaño del proyecto implantado.		M	La demostración se llevará a cabo como parte de los procedimientos de calificación de ofertas
7	La empresa debe proveer un listado de otros clientes en el país donde se haya instalado el mismo producto ofertado en un número de estaciones similar al ofertado y con un esquema de administración de la herramienta similar al ofertado.		M	Presentar certificaciones

Entregables

La empresa que resulte ganadora se obliga con el Banco Nacional de Fomento a entregar lo siguiente:

- Manuales y CDS originales del sistema de protección corporativo;
- Licencias de software necesarias para la implantación de la solución ofertada;
- Servicio de implantación de la solución en la red del BNF a nivel nacional;
- Instalación de actualizaciones del sistema de protección corporativo, sin costo adicional durante la validez del contrato de las licencias;
- Capacitación en el uso y administración del sistema de protección corporativo incluido en la oferta para 10 (diez) personas en al menos 2 localidades;

- Capacitación para el personal de soporte interno del BNF para solventar requerimientos de soporte de primer nivel;
- Soporte técnico telefónico y en sitio, sin costo adicional, durante la validez del contrato con los siguientes criterios:
    - Se incluirá 100 horas de soporte post-implantación en el servicio, las que se contabilizarán por los 12 meses luego de finalizada la implantación de la solución con la aceptación de la persona delegada por el BNF.
    - Los eventos que se atenderá serán aquellos relativos al funcionamiento de la herramienta propuesta como los siguientes, aunque no limitados a:
        - Afectación masiva de estaciones por malware;
        - Corrupción de base de datos de la (s) consola (s);
        - Suspensión de servicio de antivirus en estaciones o consola;
        - Re-instalación o re-configuración de software de protección en consola;
        - Funcionamiento inestable de la solución;
        - Requerimientos de configuraciones que impliquen nuevas tecnologías no consideradas en el proyecto actual;
        - Integración con otras herramientas en el ambiente del BNF.
    - Los tiempos de respuesta serán los siguientes:
        - Soporte técnico telefónico dentro de un lapso de no más de 30 minutos a partir de la notificación del evento;
        - Soporte técnico presencial, en sitio, en uno de los sitios principales del BNF, dentro de un lapso de no más de 2 horas a partir de la notificación del evento.

Responsabilidades del BNF

Proveer a los potenciales proveedores la información adicional que se pudiera requerir para la presentación de sus respectivas propuestas.
Coordinar las actividades planificadas según los parámetros de control de cambios y paso a producción.

PRESUPUESTO REFERENCIAL

El presupuesto referencial para este proyecto es de USD$80.000,00.

NOTA DE DESCARGO

Toda la información incluida en este documento, así como la información adicional que los oferentes pudieran requerir para presentar sus propuestas es confidencial y no podrá ser revelada a terceros.

Hasta aquí los Términos de Referencia.

Anexo 1. Definiciones (v02)

Herramienta de protección de estaciones y servidores contra malware: En el documento presente, se refiere al componente de software y/o hardware propuesto por el oferente para ser instalado en el BNF, ej. Software antivirus, servidores de actualización, appliance anti-spam, etc.
Malware: (del inglés **mal**icious soft**ware**, también llamado badware o software malicioso) es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño. Se incluye en esta categoría (entre otros): virus, adware, troyanos, spyware, rootkits, etc.
Medios electrónicos: Formatos para presentar información que usa la energía electrónica o electromecánica para que los usuarios finales (o audiencia) puedan accesar al contenido. Seto es, en contraste con “medios estáticos” (principalmente impresos) que son usualmente creados electrónicamente pero no requieren de la electrónica para ser accesados por el usuario final en su forma impresa.
Memorias externas USB: El Universal Serial Bus (bus universal en serie) es un estándar que permite conectar dispositivos de memoria en puertos externos de un computador.
Solución de protección de estaciones y servidores contra malware: En el presente documento, se refiere a la combinación de hardware, software (referidas como herramientas) y servicios de instalación, configuración e integración que sean necesarias para implantar las herramientas en el BNF.
Spam: o correo basura son los mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor.
Virus informático: programa que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Aunque popularmente se incluye al "malware" dentro de los virus, en el sentido estricto de esta ciencia los virus son programas que se replican y ejecutan por sí mismos. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más "benignos", que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse, replicándose, pero algunos contienen además una carga dañina con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

Anexo 2. Localidades actuales del BNF (v02)

Las localidades donde actualmente existen oficinas del BNF y que deben ser consideradas en el presente proyecto son las siguientes:

Región	Zonal		Nombre Agencia / Oficina
Región 1	Quito	1	Quito
	Quito	2	Cayambe
	Quito	3	Chiriyacu
	Quito	4	Cotacachi
	Quito	5	El Chaco
	Quito	6	Ibarra
	Quito	7	Los Bancos
	Quito	8	Machachi
	Quito	9	Otavalo
	Quito	10	Pimampiro
	Quito	11	Tulcán
	Quito	12	El Angel
	Quito	13	San Gabriel
	Quito	14	Santo Domingo
	Quito	15	Capacitación
	Quito	16	Rumiñahui
	Riobamba	17	Alausí
	Riobamba	18	Ambato
	Riobamba	19	Baños
	Riobamba	20	Chunchi
	Riobamba	21	Echeandía
	Riobamba	22	Guaranda
	Riobamba	23	Latacunga
	Riobamba	24	Riobamba
	Riobamba	25	San Miguel de Bolivar
	Riobamba	26	Zumbahua
	Santo Domingo	27	Atacames
	Santo Domingo	28	Corazón
	Santo Domingo	29	El Empalme
	Santo Domingo	30	Esmeraldas
	Santo Domingo	31	La Maná
	Santo Domingo	32	Limones

Región	Zonal		Nombre Agencia / Oficina
	Santo Domingo	33	Muisne
	Santo Domingo	34	Pedernales
	Santo Domingo	35	Quevedo
	Santo Domingo	36	Quinindé
	Santo Domingo	37	Tululbí
	Santo Domingo	38	Concordia
	Santo Domingo	39	El Carmen
	Santo Domingo	40	San Lorenzo
	Puyo	41	Baeza
	Puyo	42	Dayuma
	Puyo	43	Lago Agrio
	Puyo	44	Macas
	Puyo	45	Palora
	Puyo	46	Putumayo
	Puyo	47	Puyo
	Puyo	48	Shushufindi
	Puyo	49	Sucúa
	Puyo	50	Tena
	Puyo	51	El Coca
Región 2	Guayaquil	52	Guayaquil
	Guayaquil	53	Babahoyo
	Guayaquil	54	Balzar
	Guayaquil	55	Caluma
	Guayaquil	56	Catarama
	Guayaquil	57	Cumandá
	Guayaquil	58	Daule
	Guayaquil	59	El Triunfo
	Guayaquil	60	Huaquillas
	Guayaquil	61	La Troncal
	Guayaquil	62	Milagro
	Guayaquil	63	Montecristi
	Guayaquil	64	Olmedo
	Guayaquil	65	Palestina
	Guayaquil	66	Pallatanga
	Guayaquil	67	Pegro Carbo
	Guayaquil	68	Playas
	Guayaquil	69	Puerto Ayora (Galápagos)

Región	Zonal		Nombre Agencia / Oficina
	Guayaquil	70	Puerto Baquerizo (Galápagos)
	Guayaquil	71	Puerto Villamil (Galapagos)
	Guayaquil	72	Ventanas
	Guayaquil	73	Vinces
	Guayaquil	74	Duran
	Guayaquil	75	Santa Elena
	Portoviejo	76	Bahía
	Portoviejo	77	Calceta
	Portoviejo	78	Chone
	Portoviejo	79	Flavio Alfaro
	Portoviejo	80	Jipijapa
	Portoviejo	81	Paján
	Portoviejo	82	Portoviejo
	Portoviejo	83	Manta
	Machala	84	Arenillas
	Machala	85	Machala
	Machala	86	Naranjal
	Machala	87	Piñas
	Machala	88	Zaruma
	Machala	89	Santa Rosa
	Cuenca	90	Azogues
	Cuenca	91	Cañar
	Cuenca	92	Cuenca
	Cuenca	93	Girón
	Cuenca	94	Gualaceo
	Cuenca	95	Gualaquiza
	Cuenca	96	Limon Indanza
	Cuenca	97	Paute
	Cuenca	98	Mendez
	Cuenca	99	Santa Isabel
	Cuenca	100	Biblián
	Loja	101	Alamor
	Loja	102	Cariamanga
	Loja	103	Catacocha
	Loja	104	Celica
	Loja	105	Chaguarpamba

Región	Zonal		Nombre Agencia / Oficina
	Loja	106	Gonzanamá
	Loja	107	Loja
	Loja	108	Macara
	Loja	109	Pindal
	Loja	110	Saraguro
	Loja	111	Sozoranga
	Loja	111	Yantzasa
	Loja	112	Zapotillo
	Loja	113	Zumba
	Loja	114	Zamora
	Loja	115	Catamayo