

**ANEXO – CONDICIONES TÉCNICAS ESENCIALES PARA LA
PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN (FCT)**

Fecha 18/11/2014

1. DENOMINACIÓN DEL BIEN O SERVICIO

Suministro de licenciamiento de software de protección de seguridad informática para servidores y equipos de usuario final para el Instituto Colombiano de Bienestar Familiar (ICBF).

**2. CÓDIGO ESTÁNDAR DE PRODUCTOS Y SERVICIOS DE NACIONES UNIDAS
(UNSPSC, V.14.080)**

Código UNSPSC 43233200 – Software de Seguridad y Protección

3. UNIDAD DE MEDIDA

Licenciamiento de la solución para 11000 equipos de cliente final y servidores.

4. DESCRIPCIÓN GENERAL

Adquisición del licenciamiento por 3 años de una solución de software para la protección contra amenazas informáticas de servidores y equipos de usuario final del ICBF. Las actividades a realizar incluyen el suministro de licenciamiento de la solución y charlas técnicas sobre el producto adquirido.

El ICBF actualmente cuenta con un parque computacional compuesto por los servidores cuya cantidad se muestra en la siguiente tabla:

	Windows
Físicos	85
Virtuales	124
Totales:	209

Las demás licencias corresponden a computadores de usuario final, **los cuales están distribuidos así:**

Portátiles	600
Desktops	10191

5. NORMATIVIDAD APLICABLE (específica para el servicio y/o bien)

N/A

6. ESPECIFICACIONES TÉCNICAS DE LOS INSUMOS, BIENES, PRODUCTOS, OBRAS O SERVICIOS A ENTREGAR

La solución debe cumplir con las siguientes especificaciones mínimas:

6.1. Especificaciones Técnicas Generales:

- ✓ Contar con los siguientes módulos los cuales deben ser desarrollados por el mismo fabricante e integrarse para componer la solución:
 - Consola de Administración
 - Antivirus
 - Firewall de host
 - IPS/IDS(Intrusion Prevention/Detection System) para Equipos de Usuario Final
 - Control de Puertos y Dispositivos
 - Cifrado de Discos Duros y Archivos
 - Detección de vulnerabilidades (Vulnerability Assessment)
 - Control de Aplicaciones
 - Protección de Correo Electrónico en el Cliente Final
- ✓ Ser compatible con los sistemas operativos:
 - Windows server 2012
 - Windows server 2008
 - Windows Server 2003
 - Windows 8 y 8.1
 - Windows 7
 - Windows XP
- ✓ Proteger ambientes virtualizados:
 - Citrix
 - Hyper-V
- ✓ Proporcionar reportes:
 - Para cada módulo
 - Personalizables
 - Exportables a formatos pdf y csv
 - Que incluyan mínimo los siguientes: Actividad de Malware y Virus, Estado de la Red, Top de Equipos infectados, Top de malware más detectados, Estado de Protección de los Equipos, Aplicaciones Bloqueadas, Actividad del Firewall, Estado de Actualización.
- ✓ Permitir ejecutar la actualización:

- De versiones, motores y firmas de forma centralizada.
- De versiones, motores y firmas fuera de la red del ICBF.
- ✓ Permitir configurar mensajes personalizados para reportar eventos en el cliente final.
- ✓ Generar logs de eventos, alarmas y actividades compuestos por mínimo los campos de nombre de host, hora, fecha y descripción.
- ✓ Funcionalidades:
 - Contar con funcionalidad de descubrimiento de red
 - Contar con funcionalidad de instalación remota de clientes y agentes y desinstalación automática y remota de software de protección previamente instalado en los equipos.

6.2. Especificaciones de la Consola de Administración

- ✓ Permitir la creación de perfiles de usuarios de administración
- ✓ Asignar niveles de acceso a cada perfil, teniendo como mínimo los niveles de administrador, monitoreo, consultor de eventos, generación de reportes y supervisión.
- ✓ Permitir administrar y renovar las licencias adquiridas para la solución.
- ✓ Permitir realizar descubrimiento de red e instalación remota de agentes y software de cliente final.
- ✓ Permitir desinstalar automáticamente el software de cliente final de soluciones previas que impidan la instalación y correcto funcionamiento de la nueva solución.
- ✓ Alertar cuando se esté alcanzando el número de licencias adquiridas.
- ✓ Permitir la administración de todos los módulos que componen la solución de manera centralizada.
- ✓ Permitir acceso a la consola de forma local y remota.

6.3. Especificaciones del Antivirus

- ✓ Permitir realizar scan de todos los archivos de los hosts, incluyendo los contenidos de archivos comprimidos y archivos de sistema.
- ✓ Realizar escaneos por demanda y escaneos programados.
- ✓ Contar con la posibilidad de configurar excepciones para el scan de archivos en los hosts.

6.4. Especificaciones del Firewall de Host

- ✓ Permitir la configuración de reglas de tráfico con parámetros mínimos de IP de origen y destino, puertos TCP y UDP, aplicación y acción a tomar con el paquete (bloquear o permitir).
- ✓ Contar con zonas de seguridad para conexiones dentro y fuera de la red corporativa.
- ✓ Generar logs con campos mínimos de IP origen y destino, fecha, hora, puerto TCP o UDP y evento relacionado.
- ✓ Permitir la configuración de acciones (Bloquear o Permitir) sobre los paquetes TCP y UDP.

6.5. Especificaciones del IDS/IPS para Equipos de Usuario Final

- ✓ Identificar amenazas informáticas por comportamiento, en tráfico, archivos, aplicaciones, sitios web y otros.
- ✓ Permitir protección en tiempo real de los hosts.

- ✓ Analizar el tráfico de red en los equipos y generar una línea base de aplicaciones confiables.
- ✓ Detectar cambios en archivos de sistema operativo realizados por aplicaciones o procesos en el host.
- ✓ Identificar modificaciones de archivos de sistema operativo durante el inicio.
- ✓ Identificar riesgos y vulnerabilidades de día cero.
- ✓ Permitir el análisis de protocolos y servicios web, independientemente del puerto que estén usando.
- ✓ Permitir la creación de grupos para aplicación de reglas de filtrado según perfiles de usuario.
- ✓ Analizar el contenido del tráfico web para mínimo los navegadores Internet Explorer, Google Chrome y Mozilla Firefox.
- ✓ Permitir el filtrado web por reglas personalizables y por listados de reputación.

6.6. Especificaciones sobre el Control de Puertos y Dispositivos

- ✓ Permitir el control de los puertos e interfaces de los equipos con acciones mínimas de bloquear, restringir o permitir.
- ✓ Analizar y monitorear el uso de medios removibles en los hosts.
- ✓ Generar reportes de los dispositivos removibles usados en los equipos.

6.7. Especificaciones sobre Cifrado de Discos y Archivos

- ✓ Permitir el cifrado con llaves de mínimo 56 bits.
- ✓ Permitir el uso de por lo menos 2 modos de autenticación para tener acceso a la información cifrada.
- ✓ Permitir cifrar archivos en línea y fuera de línea

6.8. Especificaciones sobre el análisis de vulnerabilidades

- ✓ Analizar las aplicaciones instaladas en los hosts y reportar el nivel de cumplimiento del cliente final.
- ✓ Analizar el estado de las actualizaciones del sistema operativo y reportar la criticidad de cada detección en la consola de administración.
- ✓ Realizar escaneos por demanda o programados para detectar vulnerabilidades y reportar el nivel de riesgo de los hosts.

6.9. Especificaciones del Control de Aplicaciones

- ✓ Permitir la definición de software autorizado o denegado.
- ✓ Identificar la información usada por las aplicaciones monitoreadas.

6.10. Protección de Correo Electrónico en el Cliente Final

- ✓ Contar con Plug-in para Microsoft Outlook 2013.
- ✓ Permitir el chequeo de correo entrante y saliente
- ✓ Chequear las url de los mensajes y verificar que no estén listadas en la base de sitios web sospechosos y de phishing.
- ✓ Permitir análisis configurable de archivos adjuntos.

6.11. Licenciamiento

- ✓ Las licencias deberán cubrir actualizaciones y renovación de versiones, firmas, motores, componentes, consola, agentes, software de cliente junto con todos los módulos que componen la solución, de forma centralizada y descentralizada en línea, durante un periodo de 3 años, para 11000 hosts entre equipos de usuario final y servidores.
- ✓ Los códigos de validación de licencias o archivos de licenciamiento deberán ser instalables o registrables en la consola de administración de la solución, deberán validar todas las licencias adquiridas y no deberán necesitar ser cambiados durante los 3 años de vigencia de las licencias para realizar actualizaciones de firmas y de versiones de productos que compongan la solución.
- ✓ En caso de requerir licencias adicionales, estas deberán poder ser cubiertas mediante el reemplazo o adición de códigos de validación o archivos de licenciamiento en la consola de administración.
- ✓ Las licencias deberán poder ser trasladadas entre equipos sean estos virtuales o físicos, servidores o equipos de usuarios finales.

6.12. Garantía y soporte

6.12.1. Soporte brindado por el Fabricante

- ✓ El licenciamiento deberá incluir soporte técnico y operativo provisto por el fabricante de la solución en modalidad 7x24x365 (7 días a la semana por 24 horas al día por 365 días al año) durante los 3 años de vigencia de la licencia suministrada. Dicho soporte puede ser brindado de forma remota, alcanzable mínimo mediante e-mail y línea telefónica de atención y soporte.

7. OBLIGACIONES DEL CONTRATISTA

7.1. Obligaciones específicas

- 7.1.1. La solución suministrada por el Contratista deberá haber sido evaluada por laboratorios especializados en seguridad como AV-Test, AV-Comparatives u otros en el año 2013 o posterior, y haber alcanzado índices de detección de software malicioso de mínimo 98%.
- 7.1.2. El Contratista deberá suministrar una suscripción de licenciamiento de la solución válido por un periodo de 3 años, para un total de 11000 hosts entre servidores y equipos de usuario final.

7.1.3. En caso de requerirse licenciamiento especial o adicional para el cifrado de discos duros, este deberá cubrir solo los computadores portátiles listados en el numeral 4 – Descripción General.

7.1.4. El Contratista se compromete a hacer entrega de certificación de activación de los códigos de las licencias o archivos de licenciamiento y servicios adquiridos mediante el presente proceso.

7.1.5. El Contratista se obliga a brindar charlas técnicas para seis (6) personas seleccionadas por la Subdirección de Recursos Informáticos del ICBF, en los módulos que componen de la solución, dentro de la cual se entrega el correspondiente certificado de asistencia al curso. Donde la capacitación será presencial de 20 horas, en sesiones de 4 horas impartidas en la sede del ICBF ubicada en la Calle 57 No. 16-35 en Bogotá.

7.1.6. Las charlas técnicas deberán comprender mínimo los siguientes temas:

- Descripción de los componentes de la solución
- Requisitos y pasos de instalación de módulos, consola y base de datos
- Instalación de licencias
- Descubrimiento de red e instalación de agentes y software de cliente final.
- Backup y recovery de la solución
- Gestión de la solución usando la consola de administración
- Generación de Reportes
- Troubleshooting de módulos, componentes y software de cliente final.

Los materiales de instrucción, didácticos, informativos y demás elementos necesarios para el desarrollo de las charlas técnicas serán proporcionados por el Contratista tanto en físico y como en medio magnético, y deberán estar en idioma español y/o inglés

7.1.7. El CONTRATISTA debe garantizar durante la vigencia del licenciamiento, que el ICBF cuente con las últimas versiones del software adquirido inmediatamente estén disponibles en el mercado, sin que éstas le generen costo adicional.

7.1.8. Reportar por escrito al ICBF cualquier sugerencia que contribuya a la obtención de mejores resultados en el área de acción de la solución.

7.1.9. Acatar las instrucciones que imparta el Instituto para el cabal cumplimiento de las obligaciones del contrato, a través del Supervisor designado para el efecto.

7.1.10. El Contratista debe garantizar que el ICBF sea notificado mediante correos electrónicos cuando haya actualizaciones de productos disponibles.

- 7.1.11. El Contratista debe garantizar que con el licenciamiento adquirido por el ICBF, se cuente con acceso completo a la base de conocimiento del fabricante de la solución provista durante el tiempo de vigencia de las licencias.

7.2. Obligaciones generales

- 7.2.1. Reportar por escrito al supervisor del contrato cualquier sugerencia que contribuya a la obtención de mejores resultados.
- 7.2.2. Acatar las instrucciones que imparta el ICBF para el cabal cumplimiento del contrato, a través del Supervisor del contrato.
- 7.2.3. Guardar debida y completa reserva y confidencialidad sobre la información y los documentos del ICBF que tenga conocimiento o a los que tenga acceso en virtud del objeto del contrato.
- 7.2.4. Suscribir la garantía única, presentar los amparos requeridos para el cumplimiento del contrato y mantener actualizada su vigencia acorde con los términos pactados en la cláusula pertinente del contrato.
- 7.2.5. Cumplir con las obligaciones frente al Sistema de Seguridad Social Integral y aportes parafiscales y presentar los recibos de pago al sistema de seguridad social (salud, pensiones y riesgos profesionales) y parafiscales (Caja de Compensación, SENA, ICBF), para efectos del pago.
- 7.2.6. Mantener los precios presentados en la oferta o resultantes de la Subasta Inversa (dependiendo de la modalidad de selección), durante el tiempo de la ejecución del contrato.
- 7.2.7. Cumplir con las obligaciones derivadas del contrato actuando con alto grado de profesionalismo responsabilidad y eficacia en la ejecución de las tareas correspondientes.
- 7.2.8. Cumplir con las demás instrucciones que le sean impartidas por el supervisor del contrato que se deriven o tengan relación con la naturaleza del mismo.
- 7.2.9. Suscribir el acta de liquidación del contrato.
- 7.2.10. Entregar al Grupo Financiero de la Dirección General el formato de autorización para abono directo en cuenta de ahorros o corriente, debidamente diligenciado y firmado, anexando certificación bancaria de la titularidad de la cuenta.

7.3. Obligaciones del Sistema Integrado de Gestión:

7.3.1. Para el eje de Política de Seguridad de la Información

En el marco de este eje, se debe tener en cuenta en los estudios previos y en el contrato las siguientes actividades – obligaciones:

7.3.1.1. El Contratista debe garantizar los procesos adecuados para la protección y confidencialidad de la información suministrada por el ICBF.

7.3.1.2. El Contratista deberá guardar la confidencialidad de toda la información del ICBF a la que tenga acceso durante el desarrollo de las actividades requeridas para cumplir el objeto de este contrato

8. ACEPTACIÓN DE LOS ELEMENTOS ADQUIRIDOS

El contratista deberá entregar al supervisor del contrato, certificación firmada por el fabricante de los derechos de uso de la solución adquirida, los códigos o archivos de licencia con vigencia de 3 años, medios magnéticos de instalación de los componentes de la solución y constancia de realización de las charlas técnicas.

El ICBF podrá realizar la aceptación de la entrega del licenciamiento y el software a través del supervisor del contrato o quien éste delegue.

9. LUGAR DE EJECUCIÓN DEL CONTRATO

Para todos los efectos el domicilio contractual será la ciudad de Bogotá.

El contratista deberá entregar los elementos adquiridos en el Almacén General de la Sede de la Dirección General del ICBF, ubicado en la Av. Carrera 68 No. 64C-75, de la ciudad de Bogotá.

10. PLAZO DE EJECUCIÓN

La duración del contrato será de 10 días calendario contados a partir de la legalización del contrato. En cualquier caso esta ejecución no debe superar el 31 de diciembre de 2014.

11. FORMA DE PAGO DEL VALOR DEL CONTRATO

El valor del contrato a suscribir será hasta por el valor del presupuesto oficial, incluidos todos los costos directos e indirectos asociados al suministro de las licencias, el IVA, demás impuestos de ley.

Se pagará al contratista así:

El 90% del valor del contrato contra la entrega de la certificación firmada por el fabricante de los derechos de uso de la solución adquirida, los medios magnéticos de instalación de la solución y los códigos o archivos de licencias.

El 10% restante se pagará una vez realizadas las charlas técnicas y entregada la documentación necesaria para realizar el acta de liquidación del contrato.

Los pagos se realizarán previa presentación de la factura correspondiente, la certificación de recibo a satisfacción por parte del supervisor y la certificación del revisor fiscal o representante legal, según corresponda, sobre el cumplimiento en el pago de los aportes parafiscales y de seguridad social de sus empleados de acuerdo con lo establecido en el artículo 50 de la Ley 789 de 2002 y artículo 23 de la Ley 1150 de 2007.

El pago se realizará dentro de los **treinta (30)** días hábiles siguientes a la radicación de la factura y la certificación de cumplimiento, previa aprobación del PAC (Programa Anual Mensualizado de Caja).

Si la(s) factura(s) no ha(n) sido correctamente elaborada(s), o no se acompañan los documentos requeridos para el pago, el término para este solo empezará a contarse desde la fecha en que se presenten debidamente corregidas, o desde que se haya aportado el último de los documentos solicitados. Las demoras que se presenten por estos conceptos serán de responsabilidad del contratista y no tendrá por ello, derecho al pago de intereses o compensación de ninguna naturaleza.

Todos los pagos se realizarán conforme al PAC del Instituto Colombiano de Bienestar Familiar.

12. ANEXOS

No Aplica

13. ACEPTACIÓN CUMPLIMIENTO DE REQUERIMIENTOS TÉCNICOS

Señor proveedor o contratista potencial: Al remitir cotización y/o propuesta, usted está aceptando que la misma cumple con la totalidad de los requerimientos incluidos en el presente documento y que incluye la totalidad de costos y gastos, directos e indirectos, así como los impuestos, asociados a la ejecución del contrato. Así mismo, que en caso de resultar adjudicatario del proceso de selección correspondiente, podrá prestar el servicio y/o entregar el bien, con las condiciones técnicas descritas en el presente documento.

Elaboró	Revisó	Aprobó
Mariano Andrés Sanín Líder del Servicio de Seguridad Informática	Olga Triviño P. Líder de Contratación	Luis Felipe Onofre Subdirector de Recursos Tecnológicos