F02 - ANEXO – CONDICIONES TÉCNICAS ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DE BIEN	Fecha	26/03/13

1. DENOMINACIÓN DEL BIEN O SERVICIO

Adquisición, instalación, configuración y puesta en funcionamiento de una solución integral de seguridad que permita monitorear, auditar y proteger Aplicaciones Web, Bases de Datos y Archivos Críticos del ICBF.

2. DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO

Solución integral de seguridad que permita monitorear, auditar y proteger Aplicaciones Web, Bases de Datos y Archivos.

3. UNIDAD DE MEDIDA

Solución integral de seguridad que permita monitorear, auditar y proteger Aplicaciones Web, Bases de Datos y Archivos implementada, configurada y aceptada por el ICBF.

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

No Aplica

5. DESCRIPCIÓN GENERAL

El contratista deberá diseñar, suministrar, instalar, configurar y poner en marcha una solución integral de seguridad que permita monitorear, auditar y proteger Aplicaciones Web, Bases de Datos y Archivos Críticos que soporten la operación del ICBF.

La solución suministrada por el contratista deberá cumplir como mínimo con los siguientes requisitos:

1. Requisitos Seguridad Aplicaciones Web:

- Aprender dinámicamente los patrones de uso de las aplicaciones Web para determinar acciones anormales posteriormente de forma proactiva.

- Alertar y bloquear solicitudes hechas a las aplicaciones web que:
  a) Se desvien de los patrones de uso normales de la aplicación y la data.
  b) Intenten explotar vulnerabilidades conocidas y desconocidas.
  c) Se originen de fuentes fraudulentos y/o maliciosos
  d) Indiquen un ataque multi-stage

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

- Permitir el parcheo virtual para vulnerabilidades a nivel de aplicación a través de la integración con diferentes escáner de vulnerabilidades de aplicaciones web

- Contar con una funcionalidad Web Application Firewall (WAF) que proteja las aplicaciones de ataques como SQL Injection, Cross-site Scripting (XSS), Cross-Site Request Forgery (CSRF), entre otros.

- Analizar en tiempo real la reputación de los orígenes de las peticiones para identificar direcciones IP maliciosas y URL`s maliciosas.

- Proteger las aplicaciones web de ataque Distributed Denial of Service (DDoS).

- Generar reportes que permitan agilizar la respuesta de la Entidad frente a un incidente de seguridad así como a una investigación forense a través de análisis avanzados.

2. Requisitos Seguridad Bases de Datos:

- Auditar todos los accesos a las bases de datos con datos sensibles[1] por parte de usuarios privilegiados (conexión directa al servidor) o no privilegiados (Conexíon desde una aplicación web).

- Alertar y bloquear en tiempo real cualquier ataque a las bases de datos y aquellas solicitudes de acceso anormales.

- Detectar vulnerabilidades del software de bases de datos y realizar el respectivo parcheo virtual.

- Identificar privilegios excesivos de acceso a usuarios activos e inactivos.

- Descubrimiento automático de nuevos servidores de bases de datos dentro de la plataforma tecnológica.

- Capacidad de analizar tráfico encriptado desde y hacia las bases de datos.

- Generar reportes que permitan agilizar la respuesta de la Entidad frente a un incidente de seguridad así como a una investigación forense a través de análisis avanzados.

3. Requisitos Seguridad Archivos (Servidores de Archivos, Servidores Sharepoint, *Network Attached Storage* - NAS):

- Identificar privilegios excesivos de acceso a usuarios.

[1] Toda la información incluida en los servidores relacionados en el Anexo No. 1 es considerada sensible por la Entidad.

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

- Auditoría de acceso a todos los archivos incluyendo los accesos desde usuarios privilegiados (conexión directa al servidor) como desde aplicaciones.

- Identificar los propietarios de los datos de acuerdo a los permisos asignados a los archivos.

- Alertar y bloquear las solicitudes de acceso a archivos que no cumplan las políticas corporativas.

- Facilitar y agilizar la respuesta frente a un incidente de seguridad así como a una investigación forense a través de análisis avanzados.

4. Requisitos generales de la Solución:

- Contar con tecnología de auto-aprendizaje que permita el reconocimiento de los patrones de conducta en cuanto al uso de las Aplicaciones Web, Bases de Datos y Archivos.

- Correlacionar eventos generados en las Aplicaciones Web, Bases de Datos y Archivos que individualmente podrían no constituir un riesgo, pero que en conjunto son indicativos de una potencial violación de seguridad.

- Ser capaz de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia distintas herramientas de administración mediante protocolos SNMP y Syslog.

- Permitir la integración con la herramienta de gestión de incidentes del ICBF, para crear tickets en tiempo real cada vez que se identifique una actividad anormal en las Aplicaciones Web, Bases de Datos y Archivos. Es responsabilidad del contratista realizar dicha integración.

- Emitir alarmas y notificaciones en tiempo real vía correo electrónico al administrador de la solución o cualquier otro destinatario que considere el ICBF.

- Toda la plataforma debe ser gestionada de forma centralizada a través de una misma herramienta de administración.

- Además de soportar el protocolo de internet versión 4 (IPv4) también debe soportar IPv6.

- La solución debe disponer de un dashboard general o uno por cada línea de seguridad (Aplicaciones Web, Bases de Datos y Archivos), actualizado(s) en tiempo real para seguimiento de las actividades.

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

- Los equipos que compongan la solución deben ser compatibles con las dimensiones estándar de rack (formato 19").

- En caso de falla de un dispositivo, la solución debe garantizar de forma automática el flujo de información desde/hacía el servidor protegido mediante una funcionalidad de bypass.

- Los equipos que hagan parte de la solución deben cumplir con:

  a) Sistema de tolerancia a fallos (discos duros hot-swap, fuentes de poder redundantes y sistema de ventilación redundante),
  b) Para el monitoreo basado en red, la latencia generada debe ser menor o igual1 milisegundo.
  c) Para el monitoreo basado en agentes, el incremento en el consumo de CPU debe ser menor o igual a 2%.

Para el presente estudio de mercado:

- Se deberá realizar el diseño de la solución que satisfaga las necesidades actuales del ICBF, según lo establecido en el presente documento. Para este fin se anexa la lista de servidores a proteger (Anexo 1 – Inventario Servidores) y la Topología de Red del ICBF (Anexo 2 – Topología Red). Es importante que el dimensionamiento de la solución se haga teniendo en cuenta una proyección de crecimiento del 30% sobre el total de servidores que se encuentran en el Anexo 1 – Inventario Servidores, tomando como base el servidor con características más altas tanto de Base de datos como de Aplicaciones (ServidorBD01, ServidorApp17).
- Se deberá entregar junto con la cotización, la descripción detallada de la solución propuesta y la documentación técnica de todo el hardware y software incluido en la misma.

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

6.1. Características mínimas de la solución a entregar.

6.1.1. Seguridad para Aplicaciones Web.

a) Aprendizaje automático del comportamiento de la aplicación web y del usuario para garantizar la efectividad a la hora de detectar un ataque.

b) Contar con una completa lista de políticas y firmas de aplicaciones que permitan identificar vulnerabilidades a nivel de aplicación y entregar una completa protección.

c) Tener un servicio de seguridad basado en reputación que mitigue ataques de cualquier nivel, de acuerdo a información en tiempo real que determinen direcciones

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

IP maliciosas, direcciones de proxys anónimos, Redes The Onion Router (TOR), URL´s maliciosas y datos de geolocalización IP.

d) Detener ataques automáticos como site-scraping, DDoS, Spam y SQL Injection.

e) Identificar y detener transacciones fraudulentas a través de una aplicación web.

f) Funcionalidad de escaner de vulnerabilidades sobre el software de la aplicación y realizar parcheo virtual como plan de mitigación.

g) Proteger la aplicación web mediante la detección y control de ataques a nivel de aplicación, Web Services, servidor y red.

h) Contar con políticas de correlación de todas las solicitudes web que ayuden a reducir el número de falsos positivos.

i) Disponibilidad de reportes personalizables que contribuyan al cumplimiento de investigaciones forenses y cualquier normatividad legal.

j) Debe soportar aplicaicones web desarrolladas en lenguajes de programación disponibles en el ICBF, como: .Net, PHP, Web Logic, otros.

6.1.2. Seguridad para Bases de Datos.

a) Monitorear continuamente y de forma granular, auditando en tiempo real todas las operaciones realizadas, generando un reporte en una base de datos que muestre el “Quien, Que, Cuando, Donde y Como” para cada transacción.

b) Capturar en la base de datos propia de la herramienta todas las actividades de la base de datos tales como DML, DDL, DCL, actividades de solo lectura (SELECT), modificación de esquemas, procedimientos almacenados, triggers y objetos de la base de datos, gestión de usuarios propios de la base de datos, errores SQL y actividad de login (fallidos, exitosos).

c) Auditar el acceso tanto de usuarios que se conectan directamente al servidor como las conexiones desde distintas aplicaciones.

d) Permitir la generación de reportes consolidados y detallados de eventos auditados que cumplan con los requerimientos legales SOX, PCI DSS, HIPAA, entre otras. Estos reportes podrán ser exportados en formato PDF, HTML o CVS.

e) Alertar y bloquear en tiempo real distintos ataques a las bases de datos a niveles como Sistema Operativo, Protocolo y SQL (SQL Injection, Buffer Overflow, DoS).

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

f) Detectar actividades fraudulentas comparando la actividad monitoreada contra el patron de conducta identificado automáticamente por la herramienta.

g) Revisar los privilegios de acceso a la base de datos otorgados a los usuarios identificando permisos excesivos e innecesarios. Igualmente, se requiere detectar cuentas por defecto y cuentas con contraseñas débiles.

h) Descubrir y clasificar automáticamente la información sensible de acuerdo al uso y políticas establecidas por el ICBF.

i) Evaluar las bases de datos para determinar vulnerabilidades RDBMS, configuración de auditorías y buenas prácticas a implementar en los ambientes virtualizados. Utilizar el parcheo virtual como plan de mitigación.

j) Debe tener en cuenta las actividades desde cualquier punto (Red y Local). Eliminar los “blind-spots” utilizando agentes instalados en los servidores de Bases de Datos generando el menor impacto sobre el rendimiento del servidor.

k) Soportar las Bases de Datos desarrolladas en lenguajes disponibles en el ICBF, tales como SQL, Oracle, MySQL, otros.

6.1.3. Seguridad para Archivos (Servidores de Archivos, Servidores Sharepoint, Network Attached Storage - NAS).

a) Identificar los permisos existentes de acceso a usuarios y adelanta ciclos de revisión para garantizar que los archivos sensibles solo sean accedidos por los usuarios indicados.

b) Identificar los usuarios con privilegios de acceso excesivos. Igualmente, se requiere detectar cuentas por defecto y cuentas con contraseñas débiles.

c) Descubrir usuarios inactivos y permisos de acceso no utilizados.

d) Monitorear continuamente y de forma detallada, auditando en tiempo real todas las operaciones realizadas en los archivos que muestre el “Quien, Que, Cuando, Donde y Como” para cada acceso.

e) Generar una completa traza de auditoria que muestre el nombre de usuario, archivo accesado, directorio, operación (Abrir, Leer, Escribir, Borrar, etc), fecha y hora del acceso.

f) Provee un análisis de auditoría rápido e interactivo visualizando la actividad del archivo y los permisos de acceso del usaurio.

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

g) Alertar y bloquear en tiempo real cualquier ataque a la base de datos y aquellas solicitudes de acceso anormales.

h) Permitir la integración con usuarios y grupos de Microsoft Active Directory, LDAP y cuentas locales.

6.2. Reportes mínimos requeridos

La herramienta a suministrar deberá contar con un módulo de generación de reportes, y estar en capacidad de generar al menos los siguientes reportes:

- **Top Consultas**: Permite ver información estadística de conexión con picos en una fracción de tiempo determinado hacía los recursos de información que hacen parte del alcance (Aplicaciones Web, Bases de Datos y Archivos).
- **Equipo Origen**: Permite ver las maquinas (FQDN - Fully Qualified Domain Name o NETBIOS - Network Basic Input/Output System) que realizan conexión hacía los recursos de información que hacen parte del alcance (Aplicaciones Web, Bases de Datos y Archivos). Con este reporte se puede determinar cuáles no deberían ser permitidas.
- **Dirección IP Origen**: Al igual que "Equipo Orígen", permite ver las maquinas conectadas a los recursos de información que hacen parte del alcance (Aplicaciones Web, Bases de Datos y Archivos), pero identificadas por dirección IP.
- **Aplicación Origen**: Permite ver las aplicaciones que realizan conexión hacía las Bases de Datos. Con este reporte se puede identificar cuales aplicaciones serán permitidas y cuales no.
- **Resumen Auditoría**: Estadísticas de Auditorías realizadas en los recursos de información que hacen parte del alcance (Aplicaciones Web, Bases de Datos y Archivos).
- **Servidores Monitoreados**: El estado resumido de los servidores de aplicaciones web, bases de datos y de archivos que están siendo monitoreados.
- **Análisis de Acceso**: Permite ver todos los accesos (login) garantizados o denegados en los recursos de información que hacen parte del alcance (Aplicaciones Web, Bases de Datos y Archivos).
- **Permisos de acceso a usuarios**: Permite ver aquellos usuarios con permisos de acceso excesivos al igual que aquellos usuarios inactivos y permisos de acceso en archivos no utilizados.

La herramienta debe permitir la exportación de los reportes a al menos uno de los siguientes formatos: PDF, HTML y/o CSV.

Los reportes mencionados deberán ser entregados y parametrizados por parte del contratista en la herramienta.

De otra parte, el módulo de reportes debe ofrecer la posibilidad de generar reportes adicionales a los anteriores parametrizables por parte del usuario administrador, de todas las acciones

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

realizadas por la herramienta (medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en Aplicaciones Web, Bases de Datos y Archivos de la Entidad).

6.3. Capacitación

Se requiere que una vez finalice la implementación de la solución, el contratista realice una capacitación de al menos 40 horas, para mínimo 4 ingenieros encargados de la administración y operación de la solución, delegados por el Supervisor del Contrato, que cubra temas como instalación, configuración, administración, reportes y *troubleshooting* (solución de problemas) de la solución completa. La capacitación se dictará en la Sede de la Dirección General del ICBF en Bogotá. No es requerida la certificación de los ingenieros en la(s) herramienta(s). Se requiere certificado de asistencia emitido por el contratista para cada uno de los ingenieros que asista a la capacitación..

Todos los equipos y materiales necesarios para el curso de capacitación serán proporcionados por el contratista. El material didáctico e informativo que se proporcione para este fin deberá estar en idioma español y/o inglés.

6.4. Documentación técnica a entregar por el Contratista

El contratista deberá entregar un documento en versión impresa y digital (CD o DVD) que contenga la descripción detallada de la solución propuesta y acorde a lo requerido en el presente documento. **Para efectos del presente estudio de mercado**, este documento deberá ser entregado adjunto a la cotización.

Una vez implementada la solución, el contratista deberá entregar al supervisor del contrato la documentación técnica de todos los equipos y software suministrados, en al menos una (1) copia en medio magnético (CD o DVD). La documentación técnica deberá ser en idioma español y/o inglés de edición original del fabricante. Esta documentación debe contener como mínimo:

- Composición del sistema.
- Descripción de alarmas utilizadas por los equipos (locales y remotos), con detalles de acciones correctivas.
- Descripción de pruebas y mantenimiento preventivo, instrumentos y herramientas necesarias.
- Procedimientos operacionales para reinicio de los equipos
- Mediciones y procedimientos de administración de los equipos.
- Métodos de diagnóstico, detección y eliminación de defectos.
- Guía de comandos operacionales.
- Guía de mensajes del sistema.

6.5. Pruebas de funcionamiento y operatividad de la solución

Al término del proceso de instalación y configuración de la solución, el supervisor del contrato o quien este designe, realizará, en coordinación con el contratista, al menos las siguientes

pruebas tendientes a comprobar y garantizar el correcto funcionamiento de la solución instalada:

- Se verificará el correcto funcionamiento de los reportes mínimos requeridos por parte de la solución y que se encuentran relacionados en el ítem 6.2. Adicionalmente, se verificará que la información entregada sea consistente con base en la infraestructura objetivo.
- Se creará una Base de Datos en un ambiente de pruebas para establecer políticas que permitan evidenciar el bloqueo del acceso y la notificación al administrador de la solución.
- Se generará un reporte para mostrar el progreso de la identificación de patrones de conducta generados por la tecnología de auto-aprendizaje.
- El ICBF tomará una muestra de 2 servidores de Bases de Datos y 2 servidores de Aplicaciones incluidos en el Anexo No. 1 – Inventario Servidores y se les realizará un escaneo de vulnerabilidades aplicando el parcheo virtual como plan de mitigación.
- Se verificará que la funcionalidad de descubrimiento de nuevos servidores de bases de datos funciona correctamente.
- Se probará el sistema de tolerancia a fallos mediante prueba controlada.
- Una vez configurado, por parte del contratista, el monitoreo para los servidores del Anexo No. 1 – Inventario de Servidores, se verificará que la latencia producida por la solución en los servicios para monitoreo basado en red sea menor o igual a 1 milisegundo, y para el monitoreo basado en agentes que el incremento en el consumo de CPU producido por el agente sea menor o igual a 2%.
- Se verificará la creación de los tickets en la herramienta de gestión de incidentes del ICBF, de acuerdo con las alarmas generadas por la herramienta.

De la realización de las pruebas podrán surgir observaciones de carácter técnico las cuales deberán ser subsanadas por parte del contratista a efectos de obtener la aceptación de la solución. De los resultados satisfactorios de las pruebas y de las correcciones realizadas si hubiere lugar a estas, dependerá la aceptación de la solución por parte del supervisor del contrato.

6.6. Aceptación de los elementos y la solución adquirida

Al término del proceso de instalación y configuración de los equipos, y verificado el cumplimiento de los requerimientos técnicos establecidos en el presente documento, finalizado el curso de capacitación, y recibida la documentación técnica requerida, el supervisor del contrato elaborará el acta de aceptación de la solución, la cual será suscrita por el supervisor del contrato y el contratista.

El ICBF podrá realizar la aceptación de la entrega de los equipos a través del supervisor del contrato o quien éste delegue.

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

6.7. Garantía, provisión de repuestos y soporte técnico

El contratista deberá ofrecer una garantía sobre los equipos que componen la solución por parte del(de los) fabricante(s) de los mismos, de al menos treinta y seis (36) meses contados a partir de la fecha de aceptación de los equipos, para lo cual deberá hacer entrega al supervisor del contrato del certificado de garantía expedido por el(los) fabricantes.

El contratista deberá garantizar mediante certificación emitida por el (los) fabricante (s) de los equipos que compongan la solución, el suministro de repuestos y partes nuevas (no remanufacturadas) para los equipos instalados, de la misma marca y de iguales o superiores características a las entregadas, durante el período de.

Durante el plazo de la garantía, el contratista y/o fabricante deberá ofrecer el servicio de soporte técnico, así: El tiempo de respuesta a los requerimientos de la Entidad deberá ser de máximo de cuatro (4) horas, y deberá estar disponible 7x24.

Si se llegara a requerir el cambio de una parte, el contratista deberá realizar la instalación de la nueva parte requerida en garantía, en un tiempo no mayor a un (1) día calendario. Si no es posible contar con la nueva parte requerida, el contratista deberá garantizar el funcionamiento de los equipos por medio del suministro de forma provisional de elementos de iguales o superiores características, dentro del mismo plazo establecido (1 día) y hasta el reemplazo definitivo del elemento defectuoso. Para este caso, el tiempo de reemplazo definitivo del elemento no podrá superar los 30 días calendario a partir de la solicitud realizada por el ICBF.

El envío, instalación y configuración de los repuestos y equipos al sitio donde se encuentre configurada la solución en Bogotá será responsabilidad del contratista y no implicará costo adicional para el ICBF.

7. OBLIGACIONES DEL CONTRATISTA

7.1. Obligaciones específicas

7.1.1. Cumplir con la totalidad de especificaciones técnicas en cuanto a productos y servicios requeridos, señaladas en el presente documento.
7.1.2. Entregar en perfecto estado de funcionamiento los elementos de acuerdo con las especificaciones definidas en el presente documento y en la propuesta que hacen parte integral del contrato, empacados en sus respectivas cajas individuales, incluyendo manuales técnicos y de operación (Español o Ingles), cables, software de configuración (drivers) en medio magnético originales (si aplica), para cada uno de los componentes de los equipos.
7.1.3. Realizar la instalación y configuración de los elementos adquiridos por el ICBF, según lo señalado en el numeral 8. Lugar de ejecución del contrato, del presente documento.
7.1.4. Realizar capacitación de acuerdo con lo definido en el presente documento.

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

7.1.5. Prestar los servicios de diseño de la solución, así como la instalación, configuración y puesta en marcha de los elementos que la compongan. Estos elementos deben ser instalados en los Data Centers donde el ICBF tiene su infraestructura en Bogotá, de acuerdo con lo detallado en el Anexo No. 2 – Topología de Red.
7.1.6. Garantizar que el costo de la solución incluya todos y cada uno de los elementos, materiales y mano de obra que sean necesarios para la instalación, configuración y puesta en funcionamiento de la solución ofertada, de acuerdo con las condiciones técnicas mínimas detalladas en el presente documento.
7.1.7. Hacer entrega al supervisor del contrato del certificado de garantía del fabricante (3 años). Garantizar mediante certificación suscrita por el (los) fabricante(s) de los elementos que componen la solución, el suministro de repuestos y partes en las condiciones establecidas en el presente documento, durante el período de garantía.
7.1.8. Entregar productos originales, nuevos, no re manufacturados, de primera calidad de conformidad con las especificaciones técnicas solicitadas por el Instituto de acuerdo con el artículo 4° numeral 5° de la ley 80 de 1993.
7.1.9. Presentar la factura de los elementos suministrados, incluyendo el detalle del valor unitario de los productos adquiridos desglosando el IVA para efecto de ingreso al almacén.
7.1.10. Asumir los costos derivados del transporte y seguros de los equipos para la entrega en el almacén de la Sede la Dirección General del ICBF y posterior traslado al Data Center del ICBF, en la ciudad de Bogotá.
7.1.11. Asignar al proyecto el recurso humano idóneo y suficiente requerido para implementación de la solución.
7.1.12. Devolver al fabricante los Residuos Electrónicos generados durante la instalación y configuración de los elementos adquiridos de acuerdo a la Resolución 1512 de 2010 de MAVDT.
7.1.13. Realizar las adecuaciones lógicas y físicas necesarias para poner en marcha la solución. El ICBF realizará las adecuaciones necesarias sobre los equipos que serán monitoreados por la solución.

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 Instituto 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,

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co

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.

8. 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 Avenida Carrera 68 No. 64C-75, de la ciudad de Bogotá.

El contratista deberá instalar y configurar los elementos adquiridos en los Data Center donde el ICBF tiene su infraestructura en Bogotá, de acuerdo con el Anexo No. 2 – Topología de Red.

Las actividades de instalación y pruebas del software y hardware, se efectuarán en los Data Center donde el ICBF tiene su infraestructura en Bogotá, de acuerdo con el Anexo No. 2 – Topología de Red.

Las capacitaciones y reuniones entre el ICBF y el contratista, se efectuarán en la Sede de la Dirección General del ICBF.

9. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de hasta **90 días calendario**, contados a partir de la suscripción del acta de iniciación, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, y no podrá superar el 31 de diciembre de 2013.

10. VALOR Y FORMA DE PAGO

El valor del contrato a suscribir será hasta por el valor resultante de la adjudicación, incluidos todos los costos directos e indirectos asociados al suministro de los bienes y/o prestación del servicio, el IVA, demás impuestos de ley.

Se pagará al contratista 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, de la siguiente manera:

- Se realizara el pago del cien por ciento (100%) del valor del contrato, previa entrega por parte del proveedor de los elementos instalados y configurados, de la capacitación, documentación y de la aceptación formal a satisfacción de los mismos por parte del supervisor del contrato.

El pago se realizará dentro de los treinta (30) días hábiles siguientes a la radicación de la factura acompañada de las certificaciones requeridas, 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.

11. ANEXOS

11.1. Anexo 1 – Inventario Servidores
11.2. Anexo 2 – Topología Red

12. CERTIFICACIÓN (a suscribir por parte de los oferentes)

_____ (Nombre del proponente en caso de persona natural o del Representante Legal y/o apoderado en caso de persona jurídica), identificado con C.C No. _____, en mi calidad de representante legal y/o Apoderado de _____ (Razón Social de la empresa), identificada con NIT _____, manifiesto con la presentación y firma del presente documento que he leído, entiendo y puedo garantizar el cumplimiento total de las especificaciones técnicas contenidas en el y en caso de resultar adjudicatario me comprometo a cumplirlo en su totalidad.

_____
Firma Representante Legal y/o Apoderado
Nombre: _____
C.C. _____

Sede de la Dirección General
Avenida carrera 68 No. 64c – 75. PBX: 437 76 30
Línea gratuita nacional ICBF 01 8000 91 8080
www.icbf.gov.co