"Adquisición, instalación, configuración y puesta en funcionamiento de una solución común e integral de seguridad que contenga Firewall de Aplicaciones Web, Firewall de Bases de Datos y Firewall de Archivos, orientada a la protección de la información sensible (estructurada y no estructurada) del ICBF, mediante procesos de auditoría, control de acceso y protección de ataques externos e internos."

DOCUMENTO DE OBSERVACIONES RECIBIDAS DURANTE EL ESTUDIO DE MERCADO

ABRIL DE 2013

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

El Instituto Colombiano de Bienestar Familiar – ICBF – se permite presentar las observaciones recibidas a la **solicitud de cotización** para la Adquisición, instalación, configuración y puesta en funcionamiento de una solución común e integral de seguridad que contenga Firewall de Aplicaciones Web, Firewall de Bases de Datos y Firewall de Archivos, orientada a la protección de la información sensible (estructurada y no estructurada) del ICBF, mediante procesos de auditoría, control de acceso y protección de ataques externos e internos.

Las observaciones recibidas fueron formuladas por los siguientes interesados:

Proponente / Interesado	Representante
DIGIWARE	OCTAVIO HERNANDEZ
INTERNEXA	ALFONSO DIAZ
INDRA	HERNANDO DIAZ BELLO

A continuación se presentan las observaciones y sus respuestas:

Empresa	DIGIWARE
Representante	Octavio Hernandez

OBSERVACIÓN No. 1
Solicitamos a la entidad diligenciar el formato anexos de recolección de información para realizar el diseño la solución, es vital contar con la información detallada para generar una arquitectura consistente y una propuesta económica ajustada. Igualmetne esta información es requerida independiente del fabricante.

RESPUESTA:
Se revisaron las plantillas recibidas y se incluyó lo pertinente en la Ficha de Condiciones Técnicas y sus anexos.

OBSERVACIÓN No. 2
Solicitamos suministrar un mapa o diagrama topológico de la red en cual se incluya la conectividad y distribución física en los Switches de red de los servidores de Bases de Datos, Servidores de Aplicaciones WEB y Servidores de Archivos que se incluirán en el proyecto o permitir ir a sitio a realizar el levantamiento de la información.

RESPUESTA:
Se incluye la topología de red como anexo a la ficha técnica.

OBSERVACIÓN No. 3
Solicitamos especificar más detalladamente las cantidades de servidores tanto de base de datos como Web Servers y File Server que se incluirán en el proyecto.

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

RESPUESTA:
El Anexo No. 1 – Inventario de servidores, se dividió en tres partes: Servidores de bases de datos, Servidores de aplicaciones y Servidores de archivos/Unidad NAS, con el fin de especificar información propia para cada rol.

OBSERVACIÓN No. 4
Solicitamos para el numeral 6.1 requerimientos de "Seguridad de Bases de Datos (Database Firewall)" Se incluya que los Appliances en modo in-line incluyan interfaces de red con By-pass electrónico.

RESPUESTA:
Se considera pertinente de acuerdo a la solución requerida por el ICBF y se incluirá en la ficha técnica

OBSERVACIÓN No. 5
Solicitamos para el numeral 6.1 requerimientos de "Seguridad de Servidores de Archivos (File Firewall)" Se incluya la cantidad de usuarios que acceden a los recursos de los File Servers y de la SAN.

RESPUESTA:
Se incluyó esta variable dentro del Anexo No. 1 – Inventario servidores (Archivos).

OBSERVACIÓN No. 6
Solicitamos para el numeral 6.3 Capacitación se especifique si la capacitación es certificada o es una transferencia de conocimiento?

RESPUESTA:
No se requiere que la capacitación sea certificada, se requiere únicamente transferencia de conocimiento y certificación de asistencia. Se precisó en la Ficha Técnica.

OBSERVACIÓN No. 7
Solicitamos para el numeral 6.3 Capacitación se consideren unas 12 horas de capacitación para cada solución o funcionalidad requerida WAF, DBF y FFW.

RESPUESTA:
Se ajustó en la Ficha Técnica la cantidad de horas requeridas para la capacitación a mínimo 40 horas.

OBSERVACIÓN No. 8
Solicitamos para el numeral 6.4 Documentación técnica a entregar por el Contratista No se exija en el estudio de mercado sino en la presentación oficial de la propuesta y se defina como causal de rechazo de la propuesta no adjuntar esta documentación

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

RESPUESTA:
Se requiere la documentación técnica de los equipos que componen la solución propuesta dentro del estudio de mercado. La documentación requerida se refiere a las fichas técnicas y demás documentación soporte del diseño de la solución propuesta (no hace referencia a certificaciones de experiencia y demás documentación técnica requerida en un proceso de selección).

Las causales de rechazo serán establecidas en el pliego de condiciones y no hacen parte del estudio de mercado.

OBSERVACIÓN No. 9
Solicitamos para el numeral 6.7 Provisión de repuestos para el requerimiento "El tiempo de respuesta a los requerimientos de la Entidad deberá ser de máximo de cuatro (4) horas, 7x24. El contratista deberá realizar la instalación de las partes requeridas en garantía, dejando los equipos en perfecto estado de funcionamiento en un tiempo no mayor a un (1) día calendario." Se solicita a la entidad que se exija para este requerimiento que el proponente demuestre de manera verificable que cuenta con mínimo 1 (Un) Appliance de administración y 1 (un) Appliance de inspección de SPARE en stock para remplazar un Appliance de producción que sea afectado con un tiempo no mayor de 24 horas. Se aclara que ningún fabricante de soluciones de Seguridad se compromete a soluciones a problemas de Software o Hardware en 24 horas, esto depende del proceso de escalamiento de casos.

RESPUESTA:
El plazo establecido para cambios de partes por garantía es un requerimiento del ICBF debido a la criticidad del servicio. Cada proveedor debe establecer la estrategia que considere adecuada para cumplir con este requerimiento.

OBSERVACIÓN No. 10
Solicitamos a la entidad que en referencia al requerimiento de: *"Proteger y controlar el acceso a los repositorios de información (Servidores de archivos, NAS – Network Attached Storage, SAN - Storage Area Network, FTP - File Transfer Protocol) que contienen información crucial" especifique cuales de los repositorios contienen información crucial.*

RESPUESTA:
Toda la información almacenada en cada uno de los servidores que se encuentran en el Anexo No. 1 - Inventario de servidores, es considera crucial y sensible para el ICBF.

OBSERVACIÓN No. 11
Solicitamos a la entidad ampliar el tiempo de ejecución del proyecto de 45 días, dado que la importación, implementación y tunning de las soluciones requerirán al menos 90 días de ejecución del proyecto.

RESPUESTA:
Se considera pertinente la observación, el plazo de ejecución del contrato se amplió a 90 días.

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

OBSERVACIÓN No. 12
Dada la complejidad del proyecto, sugerimos a la entidad validar la experiencia del proveedor y de la solución en la ejecución de proyectos, solicitando adjuntar como minino tres certificaciones de proyectos ejecutados de objetos similar y del mismo fabricante ofertado.

RESPUESTA:
La experiencia mínima requerida será especificada en el pliego de condiciones.

OBSERVACIÓN No. 13
Dado que el plazo en la ejecución del proyecto requiriere extenderse, sugerimos a la entidad contemplar una forma de pago en etapas contemplando un pago inicial contra-entrega de los equipos y pago adicionales contra ejecución del proyecto.

RESPUESTA:
El supervisor del contrato expedirá la certificación de recibo a satisfacción una vez instalados, configurados y probados los equipos, la única actividad pendiente sería la capacitación de 40 horas, por lo tanto no se considera pertinente dividir los pagos.

OBSERVACIÓN No. 14
Dado la cantidad de inquietudes, solicitamos a la entidad que una vez generadas las respuestas a las mismas, se cuente con una plazo de 4 días hábiles para la presentación de las oferta

RESPUESTA:
La Entidad establecerá un nuevo plazo para la entrega de las cotizaciones, diseño de la solución y documentos soportes.

Empresa	INTERNEXA
Representante	ALFONSO DIAZ

De las características solicitadas en el documento, observamos una orientación del ICBF por la implementación de una solución que realice la protección y cuya arquitectura de implementación sea Online y además intrusiva.

Observamos en este tipo de esquemas varios aspectos

OBSERVACIÓN No. 15

Al ser un equipo Online e intrusivo, se requeriría que el administrador de la plataforma fuera muy seguramente la misma persona responsable de la base de datos, de tal manera que pueda garantizar el funcionamiento de los accesos y el servicio de la información. Motiva esto la creación de un nuevo rol dentro de la institución para este tipo de solución.

RESPUESTA:
La Subdirección de Recursos Tecnológicos cuenta con personal experto en bases de datos quienes no son los responsables directos de la base de datos. Con esto garantizamos que el administrador de la plataforma no sea la misma persona que administra las bases de datos.

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

OBSERVACIÓN No. 16

Las amplias funciones de auditoría que los equipos realizan sobre las bases de datos y el análisis de vulnerabilidades, implica que los auditores tengan también un rol de administración sobre la plataforma.

RESPUESTA:
Se resuelve esta observación con la respuesta de la Observación No. 15

OBSERVACIÓN No. 17
Los puntos anteriores implican que no haya una separación de funciones en los administradores de la solución, dado que son los que corrigen las deficiencias (vulnerabilidades y/o riesgos), pero a la vez tienen control sobre las labores de auditoría que la solución realiza

RESPUESTA:
Se resuelve esta observación con la respuesta de la Observación No. 15

OBSERVACIÓN No. 18
La localización física Online de la herramienta limita su capacidad a la posibilidad de conexión que esta tenga a los diferentes segmentos de red e incluso redes remotas para las cuales también debería ser implementada

RESPUESTA:
Se permite cubrir las limitantes planteadas con el uso de agentes de software instalados en los servidores de bases de datos para evitar puntos ciegos (blind-spots). El ICBF requiere que la solución cubra las vulnerabilidades desde cualquier vector (red y local)

OBSERVACIÓN No. 19
Con el ánimo de obtener una mejor relación costo-beneficio, un mayor aprovechamiento de las características de los productos en el mercado y un eficiente esquema para la protección de la información en el ICBF proponemos para su evaluación un esquema de conectividad como el siguiente:

El Esquema que se muestra en la anterior figura aplica para un equipo que contribuye a proteger las bases de datos de una organización, cumpliendo con las características nombradas a continuación:

Su forma de trabajo Offline permite no ser un punto de falla adicional en las conexiones entre aplicaciones y bases de datos. No hablamos entre usuarios y bases de datos por no son estos los que interactúa directamente con ellas.

RESPUESTA:
Para evitar que sea un punto de falla se requiere que la solución disponga de una funcionalidad de Bypass que dé continuidad a la operación frente a un fallo de dispositivo. Esta funcionalidad se adiciona en la ficha técnica.

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

OBSERVACIÓN No. 20
Realización de análisis de vulnerabilidades a todas las bases de datos sin importar la localización lógica dentro de la red del ICBF. Así como el descubrimiento de nuevos servidores.

RESPUESTA:
Estos requerimientos se encuentras incluidos en el numeral 5 de la ficha técnica.

OBSERVACIÓN No. 21
Revisión de niveles de cumplimiento y comparación histórica de los avances en remediación que los administradores de bases de datos ejecuten sobre los informes de vulnerabilidades que les sean reportadas

RESPUESTA:
Para realizar esta revisión se solicitan los reportes mínimos en la sección 6.2 de la ficha técnica.

OBSERVACIÓN No. 22
Total monitoreo y/o control (además de informes) sobre todas las acciones que los administradores de las bases de datos realicen sobre ellas, alertando en tiempo real sobre vulnerabilidades, cambios nocivos, fugas de información y demás

RESPUESTA:
Está incluido en la sección 6.1 Características técnicas mínimas de la solución a entregar.

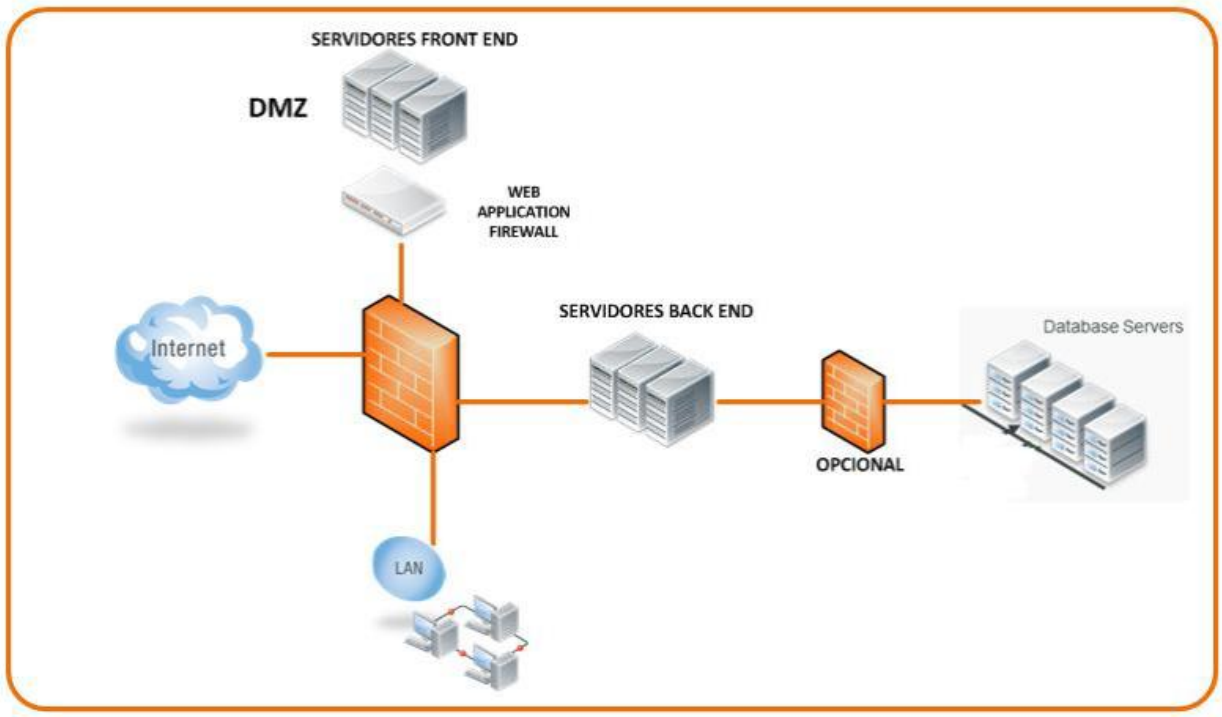
OBSERVACIÓN No. 23
Esta herramienta se convierte en un elemento fundamental para las labores de auditoría, niveles de cumplimiento y protección de la información.

Estas y otras características podemos encontrarlas en múltiples herramientas del mercado pero se parte del modelo de separación de funciones que se deben encontrar en las herramientas de seguridad.

Entendemos la importancia que para el ICBF tiene el bloqueo en tiempo real de los ataques que puedan ser objeto las bases de datos, pero todo ello es corregido partiendo de un óptimo modelo topológico que apoye a las herramientas de seguridad implementadas.

A continuación se presenta el esquema ideal que se pretende las organizaciones puedan llegar a construir:

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



La gráfica anterior muestra cómo todas las peticiones son realizadas únicamente a los servidores Front de las aplicaciones, los cuales cuentan con la protección inicial de un WAF (Web Application Firewall). Cualquier petición a los servidores BackEnd será únicamente desde los servidores Front. Así mismo cualquier petición a las bases de datos será solo permitida únicamente desde los servidores Back-end.

Los ataques hacia las bases de datos y que provengan de usuarios de internet o usuarios internos serán bloqueados por el WAF, los cuales están en total capacidad de detección y bloqueo de ataques (injección de código Sql, parametros, sentencias, etc.) Así no se realiza intervención en las sesiones hacia las bases lo cual conlleva el riesgo de daño en estas.

Con el aseguramiento frontal del tráfico realizado por el WAF y con la garantía de complimiento y aseguramiento que se hace con el equipo firewall de base de datos el ICBF realiza una amplia protección (no estar regidos a ubicación física), una eficiente protección a las aplicaciones y una excelente relación costo beneficio, sin que el instituto se enmarque en el esquema que determinada marca proponga e impida la pluralidad de los oferentes.

Con estas observaciones, solicitamos que el instituto permita a diferentes oferentes realizar presentaciones de ofertas de modelo de protección basados en lo que el ICBF actualmente posee hasta consolidar una propuesta amplia, robusta y eficiente

RESPUESTA:
El ICBF requiere la funcionalidad de bloqueo en tiempo real de ataques.

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

Empresa	INDRA
Representante	HERNANDO DIAZ BELLO

OBSERVACIÓN No. 24

SECCIÓN	*TEXTO*	*OBSERVACIONES*
5. DESCRIPCIÓN GENERAL	El contratista deberá suministrar, instalar, configurar y poner en marcha una solución común e integral de seguridad que contenga Firewall de Aplicaciones Web, Firewall de Bases de Datos y Firewall de Archivos que proteja la información sensible gestionada en los diferentes sistemas de información y repositorios de archivos que soporten la operación del ICBF.	Se solicita aclarar si las actividades de adecuación lógica y física de la red para la instalación de la solución requerida será realizada por el ICBF?

RESPUESTA:
Las adecuaciones lógicas y físicas necesarias para poner en marcha la solución de seguridad serán responsabilidad del contratista. El ICBF realizará las adecuaciones necesarias sobre los equipos que serán monitoreados por la solución.

OBSERVACION No. 25.

SECCIÓN	TEXTO	OBSERVACIONES
5. DESCRIPCIÓN GENERAL	Realizar una evaluación de todos los riesgos existentes en la infraestructura objetivo la cual se encuentra en el Anexo No.1, identificando como mínimo el nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas, configuración del sistema operativo.	Se solicita aclarar si la evaluación de riesgos debe ser realizada por la solución tecnológica solicitada ó es una información de única vez que debe entregar el oferente al momento de implementar el proyecto?

RESPUESTA:
Debe ser realizada por la solución tecnológica (herramienta suministrada) y está relacionada con el resultado del análisis de vulnerabilidades solicitado dentro de la misma.

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

OBSERVACION No. 26.

SECCIÓN	TEXTO	OBSERVACIONES
5. DESCRIPCIÓN GENERAL	Tener la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular por parte del administrador.	Se solicita aclarar si las definiciones de tipo de dato serán entregadas por el ICBF previo a las tareas de configuración y/o parametrización de la solución ofrecida?

RESPUESTA:
La clasificación de la información sensible del ICBF debe hacerla la solución tecnológica de acuerdo a los patrones de conducta que se detecten y que están relacionados con el uso de la información.

OBSERVACION No. 27.

SECCIÓN	TEXTO	OBSERVACIONES
5. DESCRIPCIÓN GENERAL	Proteger las aplicaciones web de cualquier tipo de ataque realizado desde Internet o desde la red interna, por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos y/o actividad sospechosa	Se solicita respetuosamente a la entidad entregar un diagrama de la topología de red para poder identificar los puntos donde convergen las comunicaciones para poder ubicar los equipos en la red de forma adecuada para cada una de las protecciones de aplicaciones, bases de datos y de servidores de archivos.

RESPUESTA:
Se considera pertinente la observación y se incluyó en la Ficha Técnica el Anexo No. 2 – Topología de red.

OBSERVACION No. 28.

SECCIÓN	TEXTO	OBSERVACIONES
5. DESCRIPCIÓN GENERAL	Generar análisis forenses específicos para que permitan obtener una respuesta eficaz ante los incidentes de seguridad que se presenten en el ICBF.	Se solicita respetuosamente a la entidad indicar si el análisis forense debe ser una funcionalidad o característica de las plataformas tecnológicas que protegen las aplicaciones, bases de datos y servidores de archivos o se debe presentar en modalidad de Consultoria como un servicio.

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

RESPUESTA:
No se debe presentar en modalidad de consultoría. La solución tecnológica de contribuir a la realización de análisis forense de forma ágil y precisa basado en la información recolectada.

OBSERVACION No. 29.

SECCIÓN	TEXTO	OBSERVACIONES
5. DESCRIPCIÓN GENERAL	Tener la capacidad de monitorear cualquier tipo de tráfico encriptado hacía las Bases de Datos.	Hay información y datos de los usuarios de la bases de datos que estan cifrados y que solo es posible inspeccionar alojando un certificado en el Firewall y compartirlo con la base de datos. Por lo que se informa a la entidad que la capacidad de monitorear el trafico bajo algunos escenarios no solo depende del Firewall de base de datos

RESPUESTA:
El diseño de la solución presentada por el contratista debe incluir este tipo de requerimiento externos a la solución tecnológica.

OBSERVACION No. 30.

SECCIÓN	TEXTO	OBSERVACIONES
5. DESCRIPCIÓN GENERAL	No requerir la instalación de agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.	La instalación de los agentes en algunos casos depende de la topología y son necesarios para servidores que no están centralizados o que no se puede ubicar un Firewall delante de la granja para la protección. En este caso o se ubica un Firewall adicional frente al (los) servidor(es) a proteger lo cual encarece la solución o se ubica un agente. Se solicita respetuosamente facilitar un diagrama de red para que la propuesta este basada en la realidad de la entidad.

RESPUESTA:
Se dio respuesta en la Observación No. 27.

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

OBSERVACION No. 31.

SECCIÓN	TEXTO	OBSERVACIONES
5. DESCRIPCIÓN GENERAL		Se solicita respetuosamente a la entidad informar si requiere una plataforma de correlación de eventos del tipo como se conocen en el mercado como SIEM o si se considera como una funcionalidad del Firewall de aplicación, de bases de datos y de archivos.

RESPUESTA:
Se requiere como funcionalidad de la solución tecnológica.

OBSERVACION No. 32.

SECCIÓN	TEXTO	OBSERVACIONES
Especificaciones técnicas de los insumos	Toda la plataforma debe ser gestionada de forma centralizada a través de una sola herramienta de administración.	Se solicita a la entidad respetuosamente que considere que cada una de las consolas de administración de cada una de las tecnologías pueden tener características y portales independientes y que la entidad evaluee este ítem de consolas de administración centralizada de forma abierta para cada proponente y no sea de característica inhabilitante.

RESPUESTA:
El ICBF requiere que la administración de la solución tecnológica sea centralizada.

OBSERVACION No. 33.

SECCIÓN	TEXTO	OBSERVACIONES
Especificaciones técnicas de los insumos	El costo de la solución deberá incluir 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.	Se solicita a la entidad incluir el ítem del costo de los servicios o indicar si deben hacer parte del producto (Hardware)

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

RESPUESTA:
Se modificará el formato de cotización de tal forma que sea posible separar los costos de hardware, software y servicios.

OBSERVACION No. 34.

SECCIÓN	TEXTO	OBSERVACIONES
Especificaciones técnicas de los insumos		Se solicita respetuosamente a la entidad indicar si tiene un Centro de datos de contingencia y si la solución debe estar contemplada también para ese centro de datos. Esta información es necesaria para dimensionar el numero de dispositivos y servicios de la propuesta a realizar

RESPUESTA:
No se cuenta con Centro de Datos de Contingencia.

OBSERVACION No. 35.

SECCIÓN	TEXTO	OBSERVACIONES
Especificaciones técnicas de los insumos		Se solicita respetuosamente a la entidad indicar si la solución debe estar en ambiente de alta disponibilidad para cada una de las protecciones Web, Bases de datos y File Servers

RESPUESTA:
Se solicita Sistema de tolerancia a fallos (discos duros hot-swap, fuentes de poder redundantes y sistema de ventilación redundante) en cada uno de los dispositivos que componen la solución.

OBSERVACION No. 36.

SECCIÓN	TEXTO	OBSERVACIONES
6.1. Características técnicas mínimas de la solución a entregar	Capacidad de throughput de 2 Gbps.	Se solicita respetuosamente a la entidad confirmar el throughput debido a que por el numero de aplicaciones y del numero de servidores puede estar subdimensionado.

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

RESPUESTA:
Se incluye el throughput máximo generado por los servidores de archivos y aplicaciones a monitorear en el Anexo No. 1 – Inventario servidores.

OBSERVACION No. 37.

SECCIÓN	TEXTO	OBSERVACIONES
6.1. Características técnicas mínimas de la solución a entregar	Seguridad de Bases de Datos (Database Firewall) * Características del servicio Audita todos los accesos a la información confidencial, tanto de los usuarios de las aplicaciones como de los usuarios con privilegios (administradores)	Se solicita aclarar si el ICBF entregará el listado de información confidencial así como los usuarios autorizados para accederla antes de la parametrización de la solución ofrecida?

RESPUESTA:
La herramienta debe identificar la información sensible del ICBF de acuerdo a patrones de conducta relacionados con el uso de la información. Igualmente debe detectar los usuarios que acceden a los recursos y su nivel de privilegios.

OBSERVACION No. 38.

SECCIÓN	TEXTO	OBSERVACIONES
6.1. Características técnicas mínimas de la solución a entregar	Seguridad de Servidores de archivos (File Firewall) * Características del servicio Audita todos los accesos a los archivos confidenciales, tanto de los usuarios con privilegios como de los usuarios de las aplicaciones.	Se solicita aclarar si las el ICBF entregará el listado de información que se considere confidencial asi como los usuarios autorizados para accederla antes de la parametrización de la solución ofrecida

RESPUESTA:
Se da respuesta en la Observación No. 37

OBSERVACION No. 39.

SECCIÓN	TEXTO	OBSERVACIONES
7.2. Obligaciones generales	Reportar por escrito al supervisor del contrato cualquier sugerencia que contribuya a la obtención de mejores resultados con respecto a las diademas adquiridas.	Se solicita aclarar a la entidad si existe dentro de la solución requerida algún tipo de diadema que haga parte de la misma?

RESPUESTA:
No hace parte del alcance de la propuesta por lo tanto se elimina de la ficha técnica.

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

OBSERVACION No. 40.

SECCIÓN	TEXTO	OBSERVACIONES
PLAZO DE EJECUCIÓN	El plazo de ejecución del contrato será de hasta 45 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.	Se solicita a la entidad considerar que 45 días puede tardar los equipos desde que son solicitados al fabricante hasta estar en Colombia disponibles para configuración. Las etapas iniciales de Consultoria y de estructuración de las políticas, el aprendizaje del dispositivo y el afinamiento pueden ser actividades de hasta cinco (5) meses. Por lo que la limitante de Diciembre de 2013 depende directamente de la fecha de presentación de las ofertas y adjudicación de contrato

RESPUESTA:
Plazo de ejecución del contrato se extiende a 90 días calendario.

OBSERVACION No. 41.

SECCIÓN	TEXTO	OBSERVACIONES
PLAZO DE ENTREGA DE COTIZACION		Se solicita a la entidad considerar aplazar la fecha de entrega del estudio de mercado con el fin de poder entregar una propuesta de alto nivel que sea benéfica para la entidad en el proceso posterior al estudio de mercado.

RESPUESTA:
La Entidad establecerá un nuevo plazo para la entrega de las cotizaciones, diseño de la solución y documentos soportes.

OBSERVACIONES SESIÓN DE TRABAJO PÚBLICA ENERO 23 DE 2013

OBSERVACION No. 42.

El hecho de solicitar una solución que administre la plataforma implica que sea un solo el fabricante de todas las herramientas?

RESPUESTA:
No, existen herramientas que integran la administración de diferentes dispositivos.

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

OBSERVACION No. 43.
La herramienta debe ser de alta disponibilidad? Si se requiere que la herramienta sea de alta disponibilidad, se refiere a toda la solución o parte de ella?

RESPUESTA:
Se solicita Sistema de tolerancia a fallos (discos duros hot-swap, fuentes de poder redundantes y sistema de ventilación redundante) en cada uno de los dispositivos que componen la solución.

OBSERVACION No. 44.
Solicitan saber físicamente donde están ubicados los equipos, el mapa de red o topología de red.

RESPUESTA:
Se incluye la topología de red como anexo a la ficha técnica.

OBSERVACION No. 45.
Revisar las razones por las cuales se está solicitando “Capacidad de *throughput* de 2 Gbps “

RESPUESTA:
Se incluye el throughput máximo generado por los servidores de archivos y aplicaciones a monitorear en el Anexo No. 1 – Inventario servidores.

OBSERVACION No. 46.
Cuantos se necesitan y donde se ubicaran los files servers y web servers

RESPUESTA:
El Anexo No. 1 – Inventario de servidores, se dividió en tres partes: Servidores de bases de datos, Servidores de aplicaciones y Servidores de archivos/Unidad NAS, con el fin de especificar información propia para cada rol.

OBSERVACION No. 47.
Se requiere que la herramienta no sea intrusiva en el aprendizaje pero tendrá que serlo durante la operación

RESPUESTA:
El ICBF requiere protección en tiempo real de cualquier ataque dirigido a las aplicaciones web, bases de datos y archivos.

OBSERVACION No. 48.

Se requieren agentes? Definirlo.

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

RESPUESTA:
Se permite cubrir las limitantes del monitoreo por red con el uso de agentes de software instalados en los servidores de bases de datos para evitar puntos ciegos (blind-spots). El ICBF requiere que la solución cubra las vulnerabilidades desde cualquier vector (red y local)

OBSERVACION No. 49.
El plazo de ejecución de 45 días es insuficiente, en ese plazo se importarán los equipos, habría que ampliar el plazo para realizar actividades de

1. Entrega del equipos
2. Capacitación
3. Aprendizaje
4. Implementación

RESPUESTA:
El plazo de ejecución del contrato se extiende a 90 días calendario. El tiempo para realizar la capacitación se extiende a mínimo 40 horas para cubrir toda la solución tecnológica.

OBSERVACION No. 50.
Verificación de contraseñas debe ser provisto por la herramienta? La identificación de vulnerabilidades no debe ser solo para bases de datos.

RESPUESTA:
La herramienta debe detectar contraseñas débiles, usuarios inactivos, usuarios por defecto y permisos de acceso establecidos.

OBSERVACION No. 51.
La forma en la que está estructurado el Anexo a la FT, da a entender que en un solo servidor hay BD, aplicaciones… Es correcta esta interpretación?

RESPUESTA:
No es general pero existen algunos casos en donde la base de datos y la aplicación coexisten en un mismo servidor. Se aclara en el Anexo No. 1 - Inventario de Servidores.

OBSERVACION No. 52.
En la solicitud de cotización dejar la opción de poder cotizar conjuntamente software y hardware como en un combo. Los servicios se deben cotizar por separado de las herramientas

RESPUESTA:
Se requiere que los costos de hardware y software estén separados.

OBSERVACION No. 53.
Incluir soporte del software.

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

RESPUESTA:
La garantía requerida para la solución es de 36 meses y debe cubrir incidentes con hardware, software y configuración.

OBSERVACION No. 54.
El número de horas de capacitación es muy bajo, se requieren por lo menos 12 horas por herramienta

RESPUESTA:
El tiempo para realizar la capacitación se extiende a mínimo 40 horas para cubrir toda la solución tecnológica.

OBSERVACION No. 55.
Aclarar que la capacitación se refiere a transferencia de conocimiento, no es una capacitación certificada

RESPUESTA:
No se requiere certificación, es transferencia de conocimiento.

OBSERVACION No. 56.
Aclarar Hyper - V

RESPUESTA:
En la nueva versión del anexo Inventario de Servidores se especificará el software HyperVisor en cada servidor virtual.

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