ANEXO – CONDICIONES TÉCNICAS ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN (FCT)	Fecha	10/10/2014

1 DENOMINACIÓN DEL BIEN O SERVICIO

Servicios bajo la modalidad de Outsourcing para la administración, gestión, monitoreo y control especializado de un Centro de Datos local propio de la entidad y de las soluciones de Almacenamiento, Respaldo, Servidores, Aplicaciones, Bases de Datos, Seguridad, valores agregados y conexos, para el Instituto Colombiano de Bienestar Familiar (ICBF).

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

81111500 Clase: Ingeniería de software o hardware
81111700 Clase: Sistemas de manejo de información MIS
81111800 Clase: Servicios de sistemas y administración de componentes de sistemas
81111900 Clase: Sistemas de recuperación de información
81112000 Clase: Servicios de datos
81112100 Clase: Servicios de internet
81112200 Clase: Mantenimiento y soporte de software
81112300 Clase: Mantenimiento y soporte de hardware de computador
81112400 Clase: Servicios de alquiler o arrendamiento de hardware de computador
81161500 Clase: Servicios de administración de acceso
81161600 Clase: Servicios de correo electrónico y mensajería
81161700 Clase: Servicios de telecomunicaciones

3 UNIDAD DE MEDIDA

Servicio

4 DESCRIPCIÓN GENERAL

4.1 INTRODUCCIÓN

EL CONTRATISTA prestará los servicios sobre la infraestructura propia del ICBF y/o suministrada por EL CONTRATISTA, Sedes, en los sitios que se enuncian en el presente documento donde hace presencia el ICBF, partiendo de una línea base y ajustándose a los cambios que se den en ésta, según la dinámica de las necesidades institucionales.

Como guía para el dimensionamiento de los servicios el ICBF presentará las proyecciones anuales de crecimiento sobre las líneas base, teniendo en cuenta que en caso de que estas

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

proyecciones no se cumplan EL CONTRATISTA deberá ofrecer y facturar el servicio según la demanda real.

La prestación de los servicios se realizará bajo el marco de referencia de las buenas prácticas como mínimo en ITIL v3, COBIT v5 y las Normas ISO 27001 e ISO 9001 en su última versión vigente.

Las actividades y obligaciones contractuales se llevarán a cabo en diferentes etapas, durante las cuales EL CONTRATISTA tendrá a su cargo obligaciones y objetivos.

La estrategia para la prestación de los servicios de infraestructura y la calidad del servicio de EL CONTRATISTA deberá contemplar el Anexo 002 - ACUERDOS DE NIVELES DE SERVICIO indicados para este contrato. La entidad podrá definir nuevos ANS o modificar los definidos en el anexo, según las necesidades del ICBF y de común acuerdo con EL CONTRATISTA en cualquier momento de la vigencia del contrato, con el fin de garantizar la óptima prestación de los servicios.

El incumplimiento de los ANS definidos por el ICBF, tendrá penalizaciones económicas, las cuales están definidas en Anexo 002 - ACUERDOS DE NIVELES DE SERVICIO. Su cumplimiento será verificado en la revisión mensual de los informes de gestión presentados para cada uno de los servicios.

EL CONTRATISTA deberá contar con la infraestructura (oficinas, recurso humano, recursos tecnológicos y de comunicaciones, etc.) necesaria para solventar la operación y atención de todos los servicios objeto de este contrato.

Para garantizar el cumplimiento de sus actividades diarias y la coordinación entre el personal de la Subdirección de Recursos Tecnológicos (SRT) y demás operadores, EL CONTRATISTA deberá suministrar a la firma del acta de inicio, 11 (Once) teléfonos móviles con tecnología 4G con planes de voz de mínimo 1000 minutos mensuales a cualquier operador telefónico nacional, plan cerrado (no debe permitir exceder los minutos al mes asignados) y plan de datos ilimitado, que permita la consulta de las herramientas de gestión y seguimiento en cualquier momento desde los móviles, estos serán suministrados a los profesionales de la Subdirección de Recursos Tecnológicos (SRT) encargados de realizar seguimiento al contrato.

El ICBF actualmente cuenta con una plataforma tecnológica en operación, que garantiza la disponibilidad permanente de servicios de comunicaciones de datos, voz, videoconferencia, correo electrónico, acceso a internet, comunicaciones unificadas, Intranet, impresión, acceso a aplicaciones, bases de datos y publicación de información en Internet para todas sus dependencias y funcionarios.

En cuanto a seguridad física proporcionada por el ICBF, el Instituto cuenta con un contrato vigente de vigilancia las 24 horas del día con supervisión permanente, adicionalmente las instalaciones son monitoreadas permanente por circuito cerrado de televisión.

Actualmente el esquema de prestación de servicios tecnológicos, se gestiona desde la Sede de la Dirección General en Bogotá, en donde está el Centro de Cómputo y un Data Center TIER III ubicado en Terremark Colombia (Zona Franca de Fontibón)...". Ubicadas en la Calle 57 No. 16 – 35 se encuentran la Dirección de Información y Tecnología (DIT), la Subdirección de Recursos Tecnológicos y la Subdirección de Sistemas Integrados de Información (SSII). La DIT y sus 2 Subdirecciones, son responsables de promover el uso de las tecnologías que hagan más eficiente el cumplimiento de la misión institucional y la utilización de los recursos físicos, humanos y financieros del ICBF; genera lineamientos y estándares técnicos y asiste a las diferentes dependencias del Nivel Nacional, Regionales, Centros Zonales y Dependencias en asuntos de su competencia; efectúa el proceso de evaluación técnica de las ofertas para las adquisiciones que se requieran para garantizar la plataforma tecnológica y desarrollo informático óptimo para soportar la operación del ICBF; establece normas y recomendaciones técnicas sobre los sistemas de información y realiza el control de calidad a los servicios que soportan dichos sistemas. Por su parte, el personal de EL CONTRATISTA es responsable de garantizar la instalación, administración, operación, mantenimiento, monitoreo y soporte de toda la plataforma tecnológica del ICBF, tanto propia, como arrendada, de acuerdo a lo expuesto en este documento.

Duración: La duración del contrato será de 10 meses y 15 días, contados a partir de la legalización del contrato. En los cuales los 15 (quince) primeros días, EL CONTRATISTA debe realizar las instalaciones iniciales indispensables de la infraestructura y recursos que requiera. En los siguientes 10 meses, EL CONTRATISTA realizará la operación y administración de los servicios contratados, garantizando la continuidad en la prestación de todos los servicios y de la plataforma tecnológica. En el último (1) mes del contrato, EL CONTRATISTA deberá realizar empalme y entrega del servicio al nuevo operador.

EL CONTRATISTA se obliga a garantizar el cumplimiento de los servicios ofertados, que deben ser como mínimo los requeridos por el ICBF.

4.2 CONSIDERACIONES GENERALES

EL CONTRATISTA adoptará para la gestión del servicio en el ICBF, las mejores prácticas de ITIL como mínimo v3, acompañando al Instituto en los procesos de implementación, actualización, capacitación de las Herramientas de Gestión y sensibilización de las gestiones durante todas las etapas del contrato. Así mismo, deberá elaborar e implementar en conjunto con el ICBF, los procesos de gestión necesarios para la entrega y soporte de los servicios. Durante el tiempo de duración del contrato, EL CONTRATISTA deberá asignar un responsable que asuma el rol ITIL para cada proceso.

Los roles para cada proceso de ITIL descrito a continuación se requieren y deben cumplir con los siguientes requisitos:

- Los profesionales asignados a cada rol deberán estar certificados ITIL v.3 o superior.
- No deben existir más de dos roles ITIL asignados a una sola persona.

Dichos roles son:

- Gestor de Cambios.
- Gestor de Incidentes.
- Gestor de Problemas.
- Gestor de Capacidad.
- Gestor de Niveles de Servicio.
- Gestor de Continuidad.
- Gestor de Disponibilidad.
- Gestor de Riesgos.

EL CONTRATISTA deberá contemplar con carácter obligatorio, los requerimientos realizados por el ICBF y debe garantizar los servicios con la calidad ofertada, la cual no puede ser inferior a la solicitada en los siguientes documentos:

- Pliego de Condiciones.
- Anexo Técnico.
- Anexos Informativos:
    - Anexo 001 - TABLA LINEAS BASE.xlsx
    - Anexo 002 - ACUERDOS DE NIVELES DE SERVICIO.xlsx
    - Anexo 003 - ETAPAS DEL PROYECTO.xlsx
    - Anexo 004 - CONSIDERACIONES-ETAPA-TRANSICION.xlsx
    - Anexo 005 - MATRIZ CHEQUEO ORGANIZACION PROYECTO.xlsx
    - Anexo 006 - PERFILES PROFESIONALES REQUERIDOS.xlsx
    - Anexo 007 - REPORTES OPERACIÓN.xlsx
    - Anexo 008 - PLATAFORMA DE TELEFONÍA IP.docx
    - Anexo 009 - EQUIPOS DE TELEFONÍA IP POR SEDE.xlsx

Los Acuerdos de Nivel de Servicio (ANS) serán los descritos en el documento **Anexo 002 - ACUERDOS DE NIVELES DE SERVICIO**, EL CONTRATISTA deberá garantizar la correcta implementación, configuración, administración y monitoreo de las Herramientas de Monitoreo y/o Gestión necesarias para su medición y certificar la no manipulación de los resultados, el acceso, la verificación y validación de los mismos. EL CONTRATISTA deberá generar un informe de ANS mensual. A partir de la verificación de este informe y mediante las herramientas de monitoreo y/o gestión, el ICBF podrá realizar los respectivos seguimientos y las penalizaciones a que haya lugar.

Para cada uno de los servicios incluidos en el presente documento, se presenta la línea base de acuerdo con las unidades definidas para cada servicio, así como su proyección de

crecimiento anual. Esta información se encuentra detallada en el **Anexo 001 - TABLA LINEAS BASE**.

El ICBF provee el licenciamiento de Software Base para todos los servicios, aplicaciones y máquinas de escritorio y servidores de su plataforma tecnológica y continuará proveyéndolo.

Dinámica para el cambio de los ANS y Línea Base de los Servicios.

Se contempla durante la etapa de operación, la revisión mensual de ANS y la revisión trimestral de la Línea Base, a través de los Comité Operativo y Ejecutivo con el fin de mantener la calidad en la operación del ICBF, realizando el análisis técnico e impacto económico de dichos cambios sobre la operación.

Si los ANS establecidos no reflejan la calidad de cada uno de los servicio requeridos por el ICBF, estos serán replanteados, validados y aplicados de común acuerdo entre ICBF y EL CONTRATISTA. Para ello, los ANS y su forma de medición, podrán ser revisados cada tres meses o cuando las necesidades del servicio así lo requieran.

Otras Consideraciones:

El ICBF podrá:

- Solicitar en cualquier momento el cambio de cualquier miembro del equipo de trabajo de EL CONTRATISTA cuando se presenten deficiencias técnicas, profesionales y de actitud en la prestación del servicio o labor a su cargo. De acuerdo a los requerimientos, exigencias y necesidades del ICBF.
- Solicitar las hojas de vida y realizar las pruebas que considere necesarias para verificar las competencias y calidad del personal de EL CONTRATISTA.
- Si lo considera conveniente, al final del contrato, podrá ofrecer opción de compra de algunos elementos de EL CONTRATISTA de común acuerdo con éste, según lo definido en la Ley de Contratación y los lineamientos establecidos por el ICBF.
- Considerar a todos los terceros, aliados y socios de negocio de EL CONTRATISTA que participen en la prestación de servicios objeto del presente documento como personal de EL CONTRATISTA, por lo cual EL CONTRATISTA será el único responsable de lo que realicen estos terceros.

4.3 ALCANCE

El alcance del proyecto se resume en los servicios relacionados a continuación, que debe proveer EL CONTRATISTA, de acuerdo a lo detallado en el presente documento, a nivel nacional:

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

- Centros de Cómputo
- Servidores
- Almacenamiento
- Respaldo
- Aplicaciones
- Bases de Datos
- Seguridad
- Gobernabilidad
- Office 365
- Herramientas de Gestión y Monitoreo
- Telefonía IP

A fin de implementar el proyecto, EL CONTRATISTA debe contemplar con carácter obligatorio los requerimientos establecidos por parte del ICBF en este documento y debe garantizar el suministro de los elementos de Hardware, Software, activos y recursos que sean detallados en el mismo y/o los que sean necesarios para el desarrollo de sus actividades.

Nota1: Los servicios descritos en el presente documento, podrán ser contratados o no dependiendo de los resultados del estudio de mercado.

Nota2: El ICBF podrá solicitar servicios adicionales por demanda, relacionados con el objeto del contrato de acuerdo con las necesidades que surjan durante la ejecución del mismo. Dichos servicios serán facturados por EL CONTRATISTA de manera independiente a la facturación mensual del contrato y podrán ser ajustados con los descuentos que se presenten por los ANS aplicados en el mismo periodo. El procedimiento para proveer servicios adicionales es el siguiente:

- Realización de la solicitud en los comités operativos, con el fin de validar y justificar la ejecución del servicio, para así proceder a su escalamiento a los comités ejecutivos donde se validará la forma de pago.
- Solicitud de cotización por parte del supervisor del contrato a EL CONTRATISTA acompañada de las especificaciones técnicas del servicio a contratar y sus ANS.
- La cotización allegada por EL CONTRATISTA deberá estar acorde a los precios del mercado y los tiempos exigidos por el ICBF. Para lo cual el ICBF podrá realizar la validación de la cotización solicitando en el mercado cotizaciones adicionales.
- La entrega del servicio para puesta en funcionamiento se realizará mediante acta por parte del supervisor del contrato, previa validación de cumplimiento integral de las validaciones técnicas solicitadas.

4.4 ETAPAS

La duración del contrato será de 10 meses y 15 días, contados a partir de la legalización del contrato.

El detalle de cada etapa y sus entregables se encuentra en el Anexo 003 - ETAPAS DEL PROYECTO, donde se encuentran descritos los productos que EL CONTRATISTA debe entregar en cada etapa, para revisión y aprobación por parte de la Interventoría y/o el supervisor.

La ejecución de este contrato se desarrollará en 3 (tres) etapas que se describen a continuación:

a) ETAPA DE TRANSICIÓN ENTRADA (15 días)

En esta etapa, EL CONTRATISTA debe planear y ejecutar el Plan de Transición de Entrada, que debe estar alineado al plan de entrega del proveedor saliente, con todos los servicios e instalaciones requeridas. EL CONTRATISTA tendrá el acompañamiento del operador actual de TI y del ICBF para realizar el empalme, migración de servicios y soluciones, ejecución de pruebas de inicio de operación de los servicios, de acuerdo con el plan a fin de recibir cada uno de los servicios y asumir su administración y operación.

Esta etapa está distribuida en las siguientes fases:

- Planeación de Transición y Diseño de la Solución (1 semana).
- Ejecución del Plan de Transición (1 semana).
- Implementación y configuración de la Herramienta de Gestión de propiedad del ICBF paralelo a la ejecución del plan de transición, afinar el montaje y configuración de ANS sobre las herramientas de gestión de mesa de servicio, monitoreo y medición de ANS de los demás servicios y contar con el equipo de trabajo necesario para operar.

EL CONTRATISTA se compromete a cumplir con los tiempos y documentos establecidos por el ICBF para el recibo a conformidad de los servicios objeto del contrato en la ETAPA DE TRANSICIÓN ENTRADA. En caso de incumplimiento por parte de EL CONTRATISTA por causas imputables al mismo, el ICBF descontará de las facturas de la ETAPA DE OPERACIÓN a razón del 100% de los días adicionales requeridos por EL CONTRATISTA para finalizar la ETAPA DE TRANSICIÓN DE ENTRADA, durante la ETAPA DE OPERACIÓN. Los descuentos se realizarán sin perjuicio de la amortización a que haya lugar por concepto de anticipo y aplicarán únicamente sobre los servicios que no estén operativos y recibidos a satisfacción por parte del ICBF al finalizar la ETAPA DE TRANSICIÓN ENTRADA. El valor a descontar por día, se establecerá proporcionalmente de acuerdo con el valor total de cada factura de la ETAPA DE OPERACIÓN.

El valor de las penalizaciones no podrá superar el 10% del valor del contrato de conformidad con lo establecido en el Título Primero del Código Contencioso Administrativo y el artículo 17 de la Ley 1150 de 2007.

b) ETAPA DE OPERACIÓN (10 meses)

En esta etapa, EL CONTRATISTA debe iniciar y garantizar la operación de todos los servicios contratados. Se iniciará la medición de ANS y seguimiento de la línea base.

Esta etapa está distribuida en las siguientes fases:

- Afinación de servicios y operación de los mismos (01 mes). En este período se hará medición y seguimiento de ANS, sin embargo no se presentarán penalizaciones por este concepto.

- Operación de los servicios, medición y penalización de ANS, seguimiento línea base (9 meses).

c) ETAPA DE TRANSICIÓN SALIDA (01 mes)

En esta etapa, EL CONTRATISTA debe planear y ejecutar el Plan de Transición de Salida (en paralelo a la etapa de operación), que debe estar alineado al plan de recepción del Operador Entrante, con todos los servicios, su documentación e instalaciones requeridas. EL CONTRATISTA realizará el acompañamiento al Operador Entrante y al ICBF para garantizar el empalme, migración de servicios y soluciones, ejecución de pruebas de inicio de operación de los servicios y entrega de documentación, de acuerdo con el plan detallado definido previamente en el Comité exclusivo para tal fin en donde se detallaran las actividades a fin de entregar cada uno de los servicios, la administración, documentación y operación. El plan debe ser aprobado por el ICBF.

Esta etapa no exime a EL CONTRATISTA de la penalización de los servicios por cumplimiento de ANS y del desarrollo normal de la operación descrito en la ETAPA DE OPERACIÓN.

4.5 SERVICIOS

4.5.1 CENTROS DE CÓMPUTO

Actualmente el ICBF cuenta con dos (2) centros de cómputo: un (1) centro de cómputo principal (en adelante denominado Data Center Externo) provisto a través

de un tercero en calidad de CO-LOCATION, en este se encuentran cuatro (4) rack en donde se ubican los equipos que requieren alta disponibilidad, las aplicaciones y bases de datos, servidores de desarrollo, pruebas y producción; adicionalmente cuenta con un centro de cómputo secundario (en adelante denominado Centro de Cómputo), ubicado en la Sede de la Dirección General del ICBF (Avenida Cra. 68 No. 64 C 75 de la ciudad de Bogotá), en este se encuentran algunos equipos de desarrollo y pruebas, y otras aplicaciones.

El Centro de Cómputo de la Sede de la Dirección General puede clasificarse como un centro de datos básico TIER I, este cuenta con control de acceso biométrico, sistema de CCTV independiente con dos (2) cámaras, aires acondicionados de precisión de 6 toneladas, sistema de extinción de incendios con agente FM200, transformador de aislamiento, UPS, piso falso, detectores de humedad, puerta de salida con barra anti pánico, pintura intumescente.

4.5.2 SERVIDORES

El ICBF cuenta con 232 servidores de los cuales 79 son físicos y se encuentran distribuidos en el Centro de Cómputo de la Sede de la Dirección General, el Data Center Externo y las 33 sedes regionales a nivel nacional. Los 153 servidores virtualizados son a través de la herramienta Hyper-V de Microsoft y se encuentran alojados en los servidores físicos ubicados en el Data Center Externo.

El ICBF se encuentra adelantando un plan de renovación tecnológica, en donde están incluidos los enclosures y sus servidores físicos, con el fin de reducir la obsolescencia.

El ICBF cuenta con el licenciamiento de todos los sistemas operativos que estos equipos utilizan.

Windows: Server 2003/ 2008/ 2012
Linux: CentOS y Red Hat

Controladores de Domino: El ICBF cuenta con una infraestructura de controladores de dominio centralizada Windows en la cual se administra toda la plataforma de Directorio Activo (DA), DHCP y DNS.

4.5.3 SEGURIDAD INFORMÁTICA

Este servicio se refiere a todas las configuraciones, instalaciones, dispositivos de red, tareas, métodos, reglas y procesos necesarios para proteger la información del ICBF contra accesos no autorizados a la información, modificación inapropiada o

tratamiento malintencionado de la misma, reducción de vulnerabilidades y protección contra virus y software dañino.

El ICBF, actualmente cuenta con cuatro Appliances provistos por el actual proveedor durante la vigencia del contrato, de marca Fortinet que incluyen Fortigate, y un Fortianalyzer para mejorar las funcionalidades de seguridad perimetral en su red y optimizar el acceso a Internet a través de autenticación con las bases de datos de Directorio Activo, implementadas en las políticas de Firewall, cuando un determinado tráfico es identificado por una política definida en el Firewall que tiene habilitada la opción de autenticación, el equipo decide si dicho tráfico es permitido o no en función del usuario del que se trate, pudiendo realizarse con este último una autenticación transparente de los usuarios que pertenezcan al Directorio Activo. La interfaz web de Fortinet permite la administración de la plataforma y una visualización completa del tráfico que circula a través de los equipos.

Con los equipos UTM (Unified threat management) Fortigate se realizan funcionalidades de gran granularidad en la configuración de la navegación, antispam, IPS, entre otros, adicionando las siguientes características:

- Antivirus
- Anti-spam
- Detección de Intrusos IDS
- Prevención de Intrusos IPS
- Application Control
- Data Loss Prevention
- WAN Optimization & Cache
- VPN Pptp, Ipsec, SSL
- Actualización automática
- E-mail Alert de eventos críticos
- Proxy y Filtrado de Navegación

El proveedor actual implemento dos clusters de seguridad perimetral (4 equipos en total) FortiGate 3040B ubicados en el Data Center Externo y Fortigate 620B ubicados en el Centro de Computo de la Sede Nacional, los equipos 3040B están configurados en modo NAT/Route, se configuró como filtro de navegación de UTM

para todo el tráfico a nivel nacional y se realizó la configuración de LACP (Link Aggregation Control Protocol) sobre tres interfaces de cobre para soportar el tráfico.

El creciente uso de internet ha impulsado al ICBF a permitir a sus proveedores, funcionarios y otras entidades gubernamentales acceder a los sistemas de información remotamente y a impulsar iniciativas como el teletrabajo, por lo cual se han configurado accesos VPN (Virtual Private Network) sobre los dispositivos descritos, para cumplir con ese requisito. Dichos accesos son tanto sitio a sitio como sitio a usuario y son protegidos mediante encripción SSL para VPN estándar y también VPN con IPSEC para los casos en donde se requiera utilizar software de telefonía a través de la conexión.

La infraestructura de red del ICBF es mayormente basada en plataforma Microsoft, lo cual ha requerido de la instalación de la solución WSUS para mantener actualizados de forma automática los sistemas operativos de servidores y computadores de usuario final. WSUS está configurado de forma distribuida, con un servidor principal ubicado en el Data Center Externo y servidores WSUS en las Sedes Regionales. Esta solución se administra desde el servidor principal (UPSTREAM) y actualmente se aprueban actualizaciones críticas y de seguridad para ser desplegadas a todos los servidores WSUS de las regionales (DOWNSTREAM) en horarios nocturnos específicos para cada regional, y desde ellos se distribuyen las actualizaciones a las computadoras y servidores clientes.

Adicionalmente, el ICBF cuenta con licenciamiento del antivirus Microsoft System Center 2012 Endpoint Protection con administración centralizada desde consola System Center Configuration Manager (SCCM), la cual permite acceso a herramientas de gestión del antivirus (in-depth) en los clientes, generación de reportes y atención de alertas. Las actualizaciones de definiciones se distribuyen mediante WSUS o mediante la consola SCCM. El ICBF tiene su solución de antivirus implementada en una topología conformada únicamente por el Sitio primario (Site Server).

4.5.4 ALMACENAMIENTO

El ICBF cuenta con una infraestructura propia de almacenamiento SAN, la cual es un Clariion CX4-240 que posee tres TIER, un TIER 0 de discos de Estado Sólido (SSD) de 200 GB, un TIER 1 de discos de Fibre Channel (FC) de 600 GB y un TIER 2 de discos SATA II de 2 TB; la conexión de los Hosts hacia el Storage se hace a través de 2 Switches de SAN marca Brocade 5001 a 8 Gbit/s.

Adicionalmente el ICBF cuenta con una NAS EMC Celerra NX4 la cual está compuesta con discos SATA II de 1 TB.

4.5.5 RESPALDOS (BACKUP)

El ICBF cuenta con una infraestructura propia de backup para realizar respaldo en cinta y en disco de los servidores de su propiedad, se tienen configuradas dos aplicaciones del fabricante EMC, las cuales son Networker 7.6.5.5 en la cual se realizan respaldos a cinta a través de una librería IBM System Storage TS3200 de medios LT04, la otra plataforma es Avamar 6.1.2-47, la cual se caracteriza por su combinación de hardware y software, esta solución permite el respaldo de información en disco, cuenta con una capacidad de almacenamiento de 3 TB y su gran ventaja es el algoritmo de duplicación el cual optimiza el uso de espacio en disco respaldando los datos iguales una única vez.

4.5.6 TELEFONÍA IP

La Telefonía IP es una solución tecnológica que sirve al ICBF para transmitir comunicaciones de voz sobre una red de datos basada en el estándar IP. Con la solución de Telefonía IP de propiedad del ICBF ha venido reduciendo los costos integrando sus aplicaciones de voz y datos sobre una única plataforma de red. Esta solución permite elevar la productividad, reducir costos operativos de la entidad mediante la convergencia de las comunicaciones; permite que todas las sedes del ICBF que cuenta con sistema de telefonía IP se puedan comunicar internamente como si fuese una única sede.

Actualmente el ICBF cuenta con una plataforma de telefonía IP propia marca NEC instalada en 238 sedes a nivel nacional y cuenta con 5537 extensiones, los servidores principales de la plataforma de telefonía IP se encuentran instalados en alta disponibilidad en el Data Center de Externo y las sedes de la entidad se encuentran conectadas a través de Gateway **Anexo 009 - EQUIPOS DE TELEFONÍA IP POR SEDE**, por otra parte, los equipos que conforman la solución cuentan con una garantía con el fabricante hasta el 22 de diciembre de 2014.

Con la implementación de la solución de telefonía IP propia, el ICBF obtiene mensualmente ahorros importantes en cuanto a cargos generados por llamadas de larga distancia nacional, esto teniendo en cuenta que actualmente los funcionarios cuando requieren comunicarse con otras sedes de la entidad a nivel nacional tan solo con levantar la bocina y marcar el número de extensión del funcionario receptor pueden hacerlo aprovechando las redes de comunicaciones de la entidad, es decir

la comunicación entre usuarios y entre sedes de la entidad no se requiere de llamadas de larga distancia como anteriormente se venía haciendo.

Por otra parte la entidad cuenta con una política de telefonía IP emitida por la Dirección de Información y Tecnología la cual pretende:

- Clarificar conceptos relacionados con el servicio de telefonía IP
- Dar lineamientos a los usuarios sobre el uso de la telefonía IP en la entidad
- Concientizar a los colaboradores de la entidad sobre el uso adecuado del sistema de telefonía IP, la cual es una herramienta fundamental para el cumplimiento de sus funciones.

4.5.7 APLICACIONES

En la actualidad el ICBF cuenta con algunas aplicaciones que atienden y apoyan las funciones laborales propias de los colaboradores del ICBF e igualmente la atención a los usuarios de los diferentes programas de la entidad, estas aplicaciones son desarrolladas internamente por el ICBF y otras por fábrica de software.

Algunas aplicaciones son accedidas las 24 horas del día durante todo el año y otras solo tienen un grado alto de usabilidad en horario laboral del ICBF, por lo que es necesario garantizar la gestión de la disponibilidad, integridad, seguimiento, control y seguridad de todas las aplicaciones del ICBF (actuales y las que se implementen durante la ejecución del contrato).

En el Anexo 001 - TABLA LINEAS BASE se relacionan la cantidad de aplicaciones con las que cuenta el ICBF, en el siguiente cuadro se ilustra la cantidad de aplicaciones por lenguaje de programación:

Lenguaje programación	N° de Aplicaciones
.NET	13
.Net - DevExpress	1
.net - Skelta - BPM	1
.net sichar, VS	1
ASP	1
HTML - ArcGis	1
Java	1
NA	1
Oracle developer forms	1
Oracle Forms y Reports	12
Oracle Portal, Java	1
PHP	4

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

Lenguaje programación	N° de Aplicaciones
Phyton	1
Portel	2
Power Builder, PHP	1
Visual Basic 3.0	1
VS Basic	5
VS C#	20
Total general	68

4.5.8 BASES DE DATOS

Las bases de datos con las que se cuenta actualmente, almacenan la información de los diferentes aplicativos que soportan la operación del ICBF, se tienen bases de datos en MySql, Oracle y SQL Server, pero en su mayoría recaen en el motor de base de datos Microsoft.

Es necesario garantizar la disponibilidad, integridad, seguridad y buen desempeño de las bases de datos de los diferentes ambientes con las que cuenta actualmente el ICBF, así como aquellas bases de datos que se adquieran durante la vigencia del contrato, que soportarán los sistemas de información del ICBF.

En el Anexo 001 - TABLA LINEAS BASE se relacionan la cantidad de bases de datos con las que cuenta el ICBF, en el siguiente cuando se desglosan según motor de base de datos.

Motor Base de datos	Cantidad de base de datos
SQL Server	90
MySQL	6
Oracle	43

4.5.9 OFFICE 365

El ICBF se apoya para la administración de sus servicios en línea, descritos en este documento en la plataforma Office 365, operando bajo infraestructura hibrida, ya que el 100% de los usuarios no se encuentran operando en la nube, razón por la cual requieren infraestructura On-premise (Infraestructura ubicada localmente, o en Data Center al servicio o propiedad del ICBF) para su correcto funcionamiento, la cual debe ser gestionada y administrada por EL CONTRATISTA.

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

4.5.9.1 Descripción de los servicios de Office 365

El ICBF cuenta con los siguientes servicios suscritos y adquiridos con la empresa Microsoft Corp, los cuales deben ser administrados por el contratista con su respectiva línea base de usuarios e infraestructura la cual está expuesta en el Anexo 001 - TABLA LINEAS BASE:

Federación: Permite la integración del Directorio activo On-Premise, con el Directorio Activo Azure de Microsoft que es la base de funcionamiento de Office 365 (Nube).

Correo Electrónico: Permite a los funcionarios del ICBF intercambiar mensajes de tipo E-Mail entre ellos y con personas o entidades externas, a través de las redes de telecomunicaciones, es una plataforma basada en Microsoft Exchange Online, y Microsoft Exchange Server 2013 completamente licenciada, con una infraestructura de servicio hibrida, es decir On-premise-Nube, apoyada por servidores que soportan los tres roles principales necesarios en esta versión de la plataforma (MailBox, CAS, y Hub Transport) y almacenamiento independiente.

Lync: Permite a los funcionarios del ICBF intercambiar mensajes, compartir archivos, presentaciones, establecer video llamadas, video conferencias con entes internos y externos que tengan el servicio LYNC, como con los servicios de mensajería gratuitos de Microsoft (Messenger, Skype). Esta plataforma esta soportada en Microsoft Lync Online y Microsoft Lync Server 2013, completamente licenciada. La infraestructura del servicio es hibrida, es decir On-premise-Nube, apoyada en servidores, conectada a la solución de video conferencia del ICBF a través de equipos Polycom.

Sharepoint: Permite tener sitios y subsitios para todas las áreas del ICBF, con el fin de tener espacios de colaboración en línea y On-Premise, albergando todo tipo de información, principalmente Office 365, cada uno de los sitios tiene reglas de seguridad las cuales principalmente se administran desde grupos de seguridad del Directorio Activo.

Yammer: Servicio en la Nube administrado bajo la consola principal de Office 365, en entorno Web conectado a los servidores de Microsoft, por ende no requiere administrar infraestructura asociada a la cantidad de usuarios que están alojados en los servicios de Office 365 Online.

4.5.10 HERRAMIENTAS DE GESTIÓN Y MONITOREO

Son el conjunto de Herramientas que permiten la Gestión, Administración y Monitoreo de toda la infraestructura Tecnológica, la mismas pueden estar incluidas en una sola solución global, o estar divididas de forma Modular, o independientes pero con interconectividad en caso de ser requerido.

Actualmente el ICBF cuenta con Herramientas para la Gestión de la Infraestructura de Almacenamiento, y licenciamiento completo de la Suite System Center.

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

- EIA/TIA 606, estándar para la administración de los sistemas de cableado estructurado.
- EIA/TIA 942, estándar para diseño e instalación de centros de datos.

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

6.1 CENTROS DE CÓMPUTO

6.1.1 Actividades a realizar en la administración del centro de cómputo de la Sede de la Dirección General

Estas son las actividades mínimas que realizará EL CONTRATISTA en el Centro de Cómputo de la Sede de Dirección General:

- Revisión periódica de tableros eléctricos regulados y no regulados del centro de cómputo.
- Ajuste de cables y circuitos eléctricos, nivelación de cargas eléctricas cuando se requieran.
- Cambios (mano de obra) de circuitos eléctricos, acometidas eléctricas, tomas, breaker, DPS, fusibles u otro elementos de los tableros eléctricos o acometidas del centros de cómputo cuando por requieran.
- Limpieza de impurezas que se acumulan bajo el piso falso.
- Aseo general del centro de cómputo de la sede de Dirección General, limpieza de rack, piso y paredes.
- Ingreso y conexión de rack nuevos cuando se requiera.
- Inspección, ajuste del sistema de tierras, aterrizaje de racks y equipos de los centros de cómputos.

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

- Conexión de equipos de cómputo o comunicaciones propiedad del ICBF o acompañamiento a proveedores para el ingreso de equipos nuevos cuando se requiera.
- Interconexión (cross conection) de fibras y cables UPS.
- Mantenimiento preventivo y/o correctivo de los equipos que se encuentran en el centro de cómputo (transformador de aislamiento, aires acondicionados, sistemas contra-incendios, tableros eléctricos)
- Identificación de servidores, equipos de cómputo y comunicaciones, así como su marquillado con nombre, dirección IP y placa de inventario, marquillado de patch panel y patch cord.
- Manejo de inventario de los todos los equipos de cómputo, comunicaciones y demás equipo que se encuentran dentro de los centros de cómputo.
- Elaboración y actualización de diagramas de red, diagramas de interconexión de equipos y diagramas unifilares
- Administración de permisos de ingreso de personal (asignación de usuarios) al centro de cómputo de Dirección General.
- Elaboración y manejo de bitácoras de registros del centro de cómputo de la sede de Dirección General.

6.1.2 Alcance

Prestar el servicio de administración del Centro de Cómputo de la Sede de la Sede de Dirección General, con el fin de alojar el hardware y soportar los aplicativos y bases de datos de desarrollo y pruebas.

EL CONTRATISTA debe aplicar en la administración del CENTRO DE CÓMPUTO de la SEDE DE LA DIRECCIÓN GENERAL las mejores prácticas para la gerencia de proyectos, aseguramiento de la calidad, seguridad y gestión de servicios de tecnología de información.

Administrar y operar la infraestructura del Centro de Cómputo de la Sede de Dirección General.

En este Centro de Cómputo residirá el hardware y software que actualmente se encuentra en operación.

El servicio de centros de cómputo debe contar con soporte, monitoreo y gestión en modalidad 7X24.

6.1.3 CENTROS DE MONITOREO Y CONTROL (NOC)

EL CONTRATISTA deberá disponer de un Centro de Monitoreo que centraliza las diversas actividades de monitoreo y control del funcionamiento de los sistemas y recursos utilizados, así como suministrar las herramientas de monitoreo y gestión que se requieran para conocer el estado de los servicios.

EL CONTRATISTA debe suministrar y administrar una herramienta de monitoreo que permita identificar la disponibilidad, desempeño, alertas, inventario de software y hardware.

6.2 SERVIDORES

EL CONTRATISTA debe realizar actividades de administración, gestión, operación, monitoreo, control y mantenimiento de la plataforma de servidores, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en estado de operación óptima la plataforma de servidores que soportan servicios, aplicaciones y bases de datos del ICBF.

EL CONTRATISTA deberá contar con el modelo de Infraestructura como Servicio (IaaS) contemplando los tres pilares básicos de la seguridad de la información (Integridad, Confidencialidad y Disponibilidad) y deberá ser facturada de acuerdo al consumo mensual de la infraestructura utilizada y bajo el ANS-SRV2 expuesto en el Anexo 001 - ACUERDOS DE NIVELES DE SERVICIO en el caso de que el ICBF desee realizar la migración de alguno de sus sistemas a Nube Privada.

6.3 SEGURIDAD INFORMÁTICA

El ICBF requiere el siguiente servicio de Seguridad Informática compuesto por las capas de seguridad, contando con los rendimientos, características, informes y demás requerimientos expuestos en el presente documento.

6.3.1 Características

EL CONTRATISTA velará por la seguridad informática del ICBF en todas sus sedes mediante el suministro, instalación, configuración, administración, monitoreo de soluciones tecnológicas, dispositivos de red y herramientas de software requeridos, así como con el estudio periódico y constante del comportamiento del tráfico en las

comunicaciones digitales del ICBF, la generación de propuestas, recomendaciones y planes de acción que corrijan las vulnerabilidades detectadas, el apoyo en la creación de lineamientos y políticas, y acatamiento de los ya establecidos en el ICBF, además del apoyo y acompañamiento a la implementación del SGSI que actualmente desarrolla el ICBF. EL CONTRATISTA realizará la administración, monitoreo, soporte, reconfiguración, reinstalación y mejoramiento de las herramientas de software y hardware de red que administren, gestionen o traten temas de seguridad informática, que actualmente sean propiedad del ICBF, se suministren como servicio y/o todas aquellas que el ICBF adquiera durante la vigencia de este contrato, y efectuará todas las labores necesarias para la corrección de vulnerabilidades así como también para la mitigación, análisis y estudios forenses de incidentes de seguridad que ocurran.
EL CONTRATISTA establecerá un calendario de actividades a desarrollar periódicamente con el fin de detectar vulnerabilidades de seguridad, configuraciones erróneas o susceptibles de mejora y uso indebido de los recursos informáticos, y trazará planes de acción en conjunto con el ICBF para aplicar las correcciones necesarias.
EL CONTRATISTA mantendrá documentación actualizada de todas las actividades, cambios, instalaciones, configuraciones, labores de administración y gestión, desarrollados en el ámbito de la seguridad informática y todas sus plataformas que lo compongan proponiendo mejoras en la infraestructura destinada a este servicio y en las políticas y procedimientos de gestión del mismo.
A continuación se describen las herramientas tecnológicas requeridas para la seguridad informática del ICBF, las cuales EL CONTRATISTA debe proveer, instalar, configurar, actualizar, monitorear, mantener y gestionar durante la vigencia del contrato. Estas herramientas pueden ser suministradas en hardware independiente para cada una o estar integradas en uno o varios dispositivos o UTMs, siempre y cuando cumplan con las condiciones exigidas en este documento.

6.3.2 Seguridad Perimetral

EL CONTRATISTA deberá suministrar, instalar, configurar, mantener, monitorear, gestionar los firewall de nueva generación, necesarios para la seguridad perimetral del ICBF. La solución debe garantizar la protección de las redes internas del ICBF contando con las interfaces de red, que permitan administrar el tráfico entre las redes del ICBF las cuales están interconectadas en topología estrella y convergen en el Data Center Externo.

El servicio de seguridad perimetral suministrado debe cumplir con los siguientes requerimientos mínimos:

- El servicio deberá estas arquitectado con Plataformas nuevas de Firewall de Nueva Generación, de propósito específico y estar en alta disponibilidad.

- El servicio deberá estar soportado con plataformas que cuenten con interfaces a 10 G, de tal forma que se puedan hacer conexiones al Switch de Core ubicado en el Data Center Externo.
- El servicio deberá estar soportado con plataformas que cuenten con todas las interfaces de red necesarias para una óptima prestación del servicio y totalmente compatibles con protocolos de última generación como IPV6.
- Se deberá garantizar este servicio tanto en el data center externo como en el centro de cómputo de la Sede de la Dirección Nacional del ICBF, contando con los mismo niveles de seguridad en ambas ubicaciones. Sin embargo, en el Data Center Externo el ICBF requiere Firewall de Perímetro y Firewall Interno, de tal forma que se garantice doble capa de seguridad perimetral y una arquitectura acorde a las mejores prácticas de seguridad. (Ver: Arquitectura Requerida)
- Este servicio deberá contar con las siguientes características de seguridad:
    - Firewall
    - IPS/IDS (Sistema de Prevención/Detección de Intrusos)
    - Control de Aplicaciones
    - Protección contra Malware Avanzado
    - AntiSpam
    - Filtrado Web
    - Data Leak Prevention
    - VPN IPSec
    - VPN SSL
- Rendimiento Mínimo de las Plataformas que soportan el Servicio Seguridad Perimetral Data Center Externo:
    - Rendimiento mínimo de Firewall : 55 Gpbs
    - Rendimiento de IPS/IDS: 14 Gbps
    - Control de aplicaciones mínimo: 15.000 Usuarios de red
    - Rendimiento de Protección contra Malware de 14 Gbps

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

- Rendimiento AntiSpam: Mínimo 4000 Cuentas de Correo
- Rendimiento Filtrado Web: Mínimo 15.000 Usuarios de red
- Rendimiento VPN IPSec: 20 Gbps
- Rendimiento VPN´s SSL: 2.000 VPN´s SSL totalmente funcionales.

- Rendimiento Mínimo de las Plataformas que soportan el Servicio Seguridad Sede Dirección Nacional del ICBF:
  - Rendimiento mínimo de Firewall : 18 Gpbs
  - Rendimiento de IPS/IDS: 5 Gbps
  - Control de aplicaciones mínimo: 2.000 Usuarios de red
  - Filtrado Web: 2.000 Usuarios de red
  - Rendimiento de Protección contra Malware de 3 Gbps

Cada una de las características de seguridad deberá permitir:

- **Funciones de Firewall de Nueva Generación**
  - Las reglas de firewall deben analizar las conexiones que atraviesen el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
  - Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario),
  - La solución será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico
  - Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis
  - La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.

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 solución soportará políticas basadas en dispositivo. Esto Significa que podrán definirse políticas de seguridad de acuerdo al dispositivo (móvil, laptop) que tenga el usuario.

- **Funciones de Protección/Detección de Intrusos IPS/IDS**
  - El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.
  - Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6.
  - Capacidad de detección de más de 3500 ataques.
  - El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos.
  - Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
  - Actualización automática de firmas para el detector de intrusos durante la duración del contrato
  - Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

- **Funciones de Control de Aplicaciones**
  - La solución debe soportar la capacidad de identificar la aplicación que origina el tráfico a partir de la inspección del mismo.
  - La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
  - La solución debe tener un listado de al menos 3000 aplicaciones ya definidas por el fabricante.
  - El listado de aplicaciones debe actualizarse periódicamente y de forma automática.

- Para aplicaciones identificadas o no identificadas deben poder permitirse, bloquearse o registrarse.
- Para aplicaciones de tipo P2P debe poder controlarse con políticas de traffic shaping.

- **Funciones de Protección contra Malware**
  - Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer análisis de Antivirus en tiempo real en al menos los siguientes protocolos: HTTP, SMTP, IMAP, POP3, FTP.
  - El Antivirus deberá poder configurarse de forma que los archivos sean totalmente reconstruidos por el motor antes de hacer la inspección garantizando que archivos que tengan compresión puedan también ser analizados.
  - Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
  - El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
  - La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.
  - El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
  - Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizados. Dicha lista debe actualizarse de forma periódica por el fabricante y automática en el equipo.

- **AntiSpam**
  - La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.

- La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
- La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM
- En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

- **Funciones de Filtrado WEB**
  - Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 70 categorías.
  - Debe poder categorizar contenido Web requerido mediante IPv6.
  - Capacidad de filtrado de scripts en páginas web (JAVA/Active X)
  - La solución de Filtraje de Contenido debe soportar el forzamiento de “Safe Search” o “Búsqueda Segura” independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad deberá estar disponible al menos para Google, Yahoo! y Bing.
  - Esta funcionalidad deberá garantizarse como mínimo para 15.000 Usuarios de la entidad.
- **Funciones de Manejo de tráfico y calidad de servicio.**
  - Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall
  - Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP, Usuario o Grupos de Usuario en forma independiente.

- Capacidad de poder definir ancho de banda garantizado en kbps por segundo para aplicaciones.

- **Funciones de VPN IPSEC**
  - Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)
  - Soporte para IKEv2 y IKE Configuration Method
  - Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES
  - Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits
  - Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
  - Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
  - Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.

- **Funciones de VPN SSL**
  - Capacidad de realizar SSL VPNs.
  - Soporte a certificados PKI X.509 para construcción de VPNs SSL.
  - Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
  - Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
  - La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS

- **Autenticación de las plataformas que soportan el servicio**
  - Capacidad de integrarse con Servidores de Autenticación RADIUS.

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

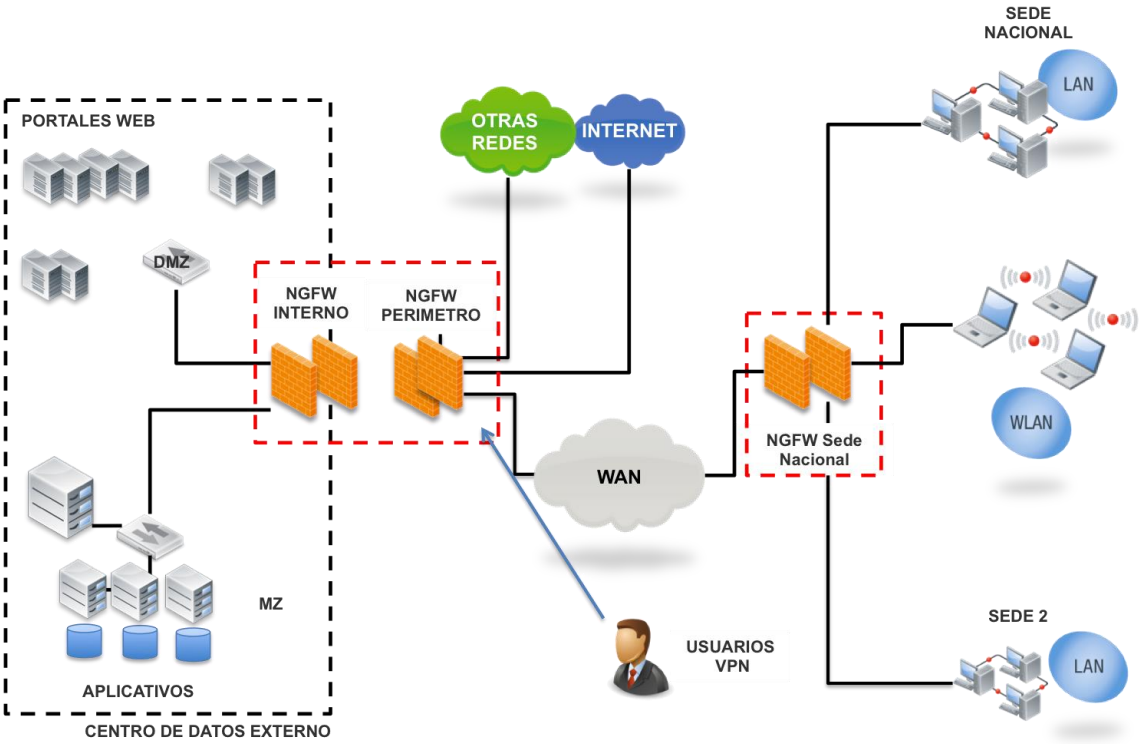
- Capacidad incluida, al integrarse con LDAP o Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password, aprovechando las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"

- **Funciones de Inspección de Contenido SSL**
  - La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
  - La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
  - El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS

- **Virtualización de la Seguridad Perimetral (Datacenter Externo)**
  - La solución ofertada para soportar el servicio deberá tener como mínimo 2 firewalls virtuales incluidos. Los cuales deberán quedar totalmente implementados y con las políticas de seguridad requeridas por el ICBF, totalmente configuradas.
  - Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red.
  - Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
  - Cada Firewall virtual deberá tener la posibilidad de administrarse por separado con usuarios, operadores y administradores por separado.
  - Cada Firewall deberá contar con todas las características de seguridad anteriormente descritas y estar configurados acorde al requerimiento de 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

***Arquitectura Mínima Requerida:**



La anterior es una arquitectura referencial, sin embargo el oferente deberá garantizar la recomendación, reconfiguración y puesta en operación de las mejores prácticas basado en los estándares de seguridad informática existentes.

6.3.3 Seguridad Avanzada de Red

EL CONTRATISTA deberá suministrar, instalar, configurar, mantener, monitorear, gestionar la solución de seguridad contra amenazas avanzadas tipo SandBox requerida para la seguridad del ICBF. La solución debe garantizar la protección de las redes internas del ICBF contra malware avanzado contando con las interfaces de red y recursos necesarios para un correcto funcionamiento.

Esta solución debe poder trabajar con la solución de seguridad perimetral del Data Center Externo y el Centro de Cómputo la Sede Nacional para la mitigación de este tipo de amenazas de acuerdo a las siguientes funcionalidades:

- **Detección Proactiva y Mitigación:**
  - Ejecución de código malicioso en sistemas operativos virtualizados.
  - Soporte de Múltiples filtros antes de la ejecución en el OS Virtual.
  - Los múltiples filtros deben incluir filtros de AV, Queries a base de datos en la nube y simulación de código independiente del Sistema Operativo.
  - Debe estar en la capacidad de detectar los siguientes tipos de infección y ataques:
    - Gusanos
    - Botnet: Archivos que actúan como un cliente de una red Bot.
    - Hijack: Archivos que tratan de modificar registros para tener acceso al sistema.
    - Stealer: Archivos que tratan de substraer información confidencial.
    - Backdoor: Archivos que tratan de instalarse como servicios nuevos de red para permitir el acceso remoto.
    - Injector: Archivos sospechosos que inyectan código en los procesos del sistema.
    - RootKit: Archivos que tratan de esconder su comportamiento funcionando en conjunto con procesos del sistema.
    - Adware: Archivos tratando de acceder a sitios web.
    - Troyanos: Archivos con un payload malicioso.
    - Riskware: Software que tiene posibles procesos que puedan poner en riesgo la infraestructura.
    - Greayware: Archivos con comportamiento similar al de virus
- **Protección Avanzada de Amenazas:**
  - La solución debe estar en la capacidad de aplicar técnicas de detección basada en comportamiento con análisis sobre ambientes Sandbox.

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

- Detección de modificación de Archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red.
- Sandbox OS Virtual: Múltiples instancias de Windows 7, Windows 8 y Windows XP completamente Licenciadas.
- Tipos de Archivos: exe, dll, PDF y Javascript. En modo integrado debe poder analizar tar, gz, tar.gz, zip, bz2, tar.bz2, bz, tar.
- Protocolos/Aplicaciones:
    - Modo Sniffer – http, ftp, pop3, imap, smtp.
    - Modo integrado con solución de seguridad perimetral: http, smtp, pop3, imap, mapi, ftp, im y sus equivalentes en SSL.
- Debe ser posible enviar los archivos a análisis en la nube para análisis manual y creación de firmas.
- Callback Detection: Botnet, C&C communication.
- La solución debe incluir un módulo de web-filtering para inspeccionar y marcar las conexiones a URL maliciosas que traten de hacer los procesos ejecutados por los archivos que se inspeccionan.
- Los archivos que son analizados con el OS Sandbox deben entregar un análisis posterior a la ejecución de las siguientes características:
    - Descarga de Virus
    - Modificación de registro.
    - Conexiones externas a IPs maliciosas.
    - Infección de procesos.
- La solución debe estar en la capacidad de procesar múltiples archivos al mismo tiempo, se debe contar con múltiples VM para el análisis de Sandbox OS.
- El resultado de los análisis debe clasificar los archivos de acuerdo al nivel de riesgo como Alto, medio o bajo. Esta clasificación se hará de acuerdo a un score y la cantidad de puntos que tenga cada archivo en su análisis.

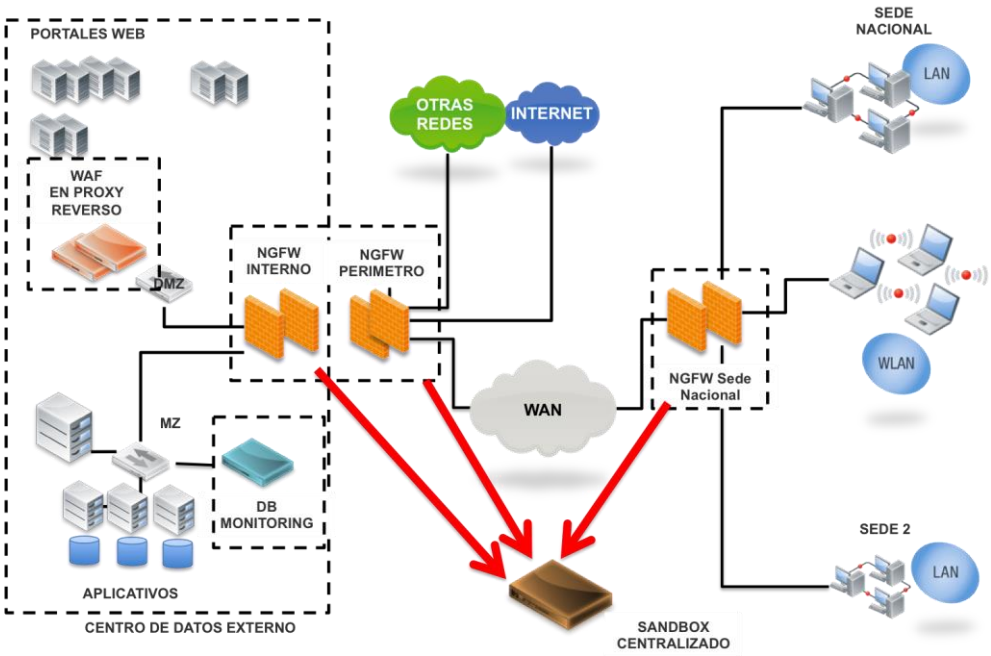
- Debe ser posible habilitar el envío de notificaciones cada vez que el análisis detecte Malware.

- **Modo de Implementación:**
  - La solución debe poderse integrar con los dispositivos de seguridad del Data Center Externo y del Centro de Computo de la Sede Nacional.
  - La solución debe poder ser implementada de una de las siguientes formas:
    - File Input: Debe ser posible manualmente hacer una subida de los archivos a analizar.
    - Sniffer: El equipo debe estar en la capacidad de recoger el tráfico de un puerto en modo espejo.
    - Integración con FW: En este modo la solución debe integrarse con los dispositivos de seguridad del Data Center Externo y el Centro de Computo de la Sede Nacional para que este le envíe archivos sospechosos para el análisis.
  - Se debe poder implementar en un ambiente distribuido donde múltiples dispositivos de seguridad perimetral le envían archivos para análisis.
  - Soporte de rutas estáticas.
  - Autorización de dispositivos que quieren enviar archivos para análisis.

- **Características**
  - La solución debe estar en la capacidad mínima de analizar en Sandbox 500 archivos por hora.
  - La Solución debe tener al menos 28 Máquinas Virtuales totalmente licenciadas.
  - Debe incluir Almacenamiento interno de 8 TB y crecimiento hasta 16 TB.
  - Fuente Redundante.
  - Al menos 4 Puertos RJ45.

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

***Arquitectura Mínima Requerida:**



6.3.4 Seguridad de Acceso a la red (NAC - Network Access Control)

EL CONTRATISTA suministrará, instalará, configurará, monitoreará y mantendrá una solución de NAC para el ICBF, evaluará y configurará las políticas de acceso a la red de común acuerdo y con la aprobación de la SRT del ICBF. La solución de NAC deberá cumplir las siguientes características mínimas:

- ✓ Implementación no descriptiva e interacción con la infraestructura de red existente con instalación fuera de banda.
- ✓ Establecer el control de acceso a la red a computadores, laptops, notebooks, tablets, y otros dispositivos móviles e inalámbricos independientemente de su sistema operativo.
- ✓ Contar con integración al Directorio Activo de Microsoft y utilizarlo para autenticación.
- ✓ Posibilitar la visibilidad de usuarios, sus dispositivos y el estado de la infraestructura de seguridad de los mismos con respecto a políticas de acceso definidas.

- ✓ Permitir la visibilidad de los dispositivos conectados a la red en tiempo real y generar reportes personalizables.
- ✓ Identificar los equipos en el momento en que ingresan a la red, clasificarlos y notificar si existen problemas de seguridad asociados a ellos, solucionarlos automáticamente y en caso de no poder hacerlo, ponerlos en cuarentena. Distinguir entre equipos autorizados, no autorizados, conocidos, desconocidos, administrados y no administrados.
- ✓ Supervisar continuamente el comportamiento de los dispositivos y bloquear ataques.
- ✓ Permitir la creación de políticas de acceso administrables y configurables para bloquear, aislar y reparar los dispositivos que no cumplan con las políticas de acceso sin necesitar de la atención de un administrador de red.
- ✓ Garantizar que los dispositivos que se conectan a la red del ICBF por distintos medios como RED DE AREA LOCAL (LAN) , RED INALAMBRICA (WLAN) y VPN, cumplan con los requisitos de acceso establecidos y aplicarles las políticas definidas, servicios de remediación y cuarentena.
- ✓ Supervisar el comportamiento de los dispositivos para detectar amenazas y actividad de software malicioso.
- ✓ Permitir el registro de invitados y garantizar su acceso sin poner en riesgo la seguridad de la red.
- ✓ Controlar la conexión de todas las computadoras del ICBF y soportar el crecimiento del parque computacional durante la vigencia del contrato
- ✓ Administración centralizada con consola de administración accesible vía web.

6.3.5 Seguridad en Aplicaciones WEB

EL CONTRATISTA deberá suministrar, instalar, configurar, mantener, monitorear, gestionar los Firewall de Aplicaciones necesarios para la seguridad de las aplicaciones Web del ICBF. La solución debe garantizar la protección de los aplicativos web que el ICBF tenga publicados en Internet, Intranet y la WAN de la entidad.

El servicio de seguridad en aplicaciones web debe cumplir con los siguientes requerimientos mínimos:

El servicio deberá estar arquitectado con Plataformas nuevas de Firewall de Aplicaciones Web, de propósito específico y estar en alta disponibilidad, Por temas de

desempeño, estas plataformas solo deberán tener este rol de protección de aplicaciones.

El servicio deberá estar soportado con plataformas que cuenten con interfaces a 10 G, de tal forma que se puedan hacer conexiones al Switch de Core del Data center Externo en caso de ser necesario.

El servicio deberá estar soportado con plataformas que cuenten con todas las interfaces de red necesarias para una óptima prestación del servicio y totalmente compatibles con protocolos de última generación como IPV6.

Se deberá garantizar este servicio en las aplicaciones Web alojadas en el Data Center externo del ICBF. (Ver: Arquitectura Mínima Requerida)

Este servicio deberá contar con las siguientes características de seguridad:

- Firewall de Aplicaciones Web especializado
- Protección AntiDefacement
- Proteccion DoS
- AutoAprendizaje de las Aplicaciones Web
- AntiMalware en HTTP
- Contención de Ataques Basado en Geolocalización
- Análisis de Vulnerabilidades en Aplicaciones Web

Rendimiento Mínimo de las Plataformas que soportan el Servicio Seguridad en aplicaciones Web:

- Rendimiento HTTP mínimo de 4 Gbps.
- Rendimiento mínimo de nuevas conexiones http por Segundo: 90.000
- Rendimiento Mínimo de Conexiones Concurrentes: 600.000
- Rendimiento HTTPS mínimo de 1Gbps
- Mínimo de aplicaciones web a proteger y que deben entregarse aseguradas con el WAF: 10

Cada una de las características de seguridad deberá permitir:

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

- **Firewall de aplicaciones web**

Deberá integrar firmas de amenazas y ataques conocidos y deberá proteger de ataques nuevos o de día cero actualizándose durante el tiempo del proyecto.

- Cross-Site Scripting (XSS)
- SQL Injection
- Remote File Inclusion
- Local File Inclusion
- OS Commands
- Troyanos y virus
- Exploits
- Información Sensible del servidor
- Fugas de Información
- Firmas personalizadas

Deberá proteger de las siguientes amenazas:

- Adobe Flash Binary (AMF) protocol Attack.
- Botnet
- Browser Exploit Against SSL /TLS
- Brute Force Login Attack
- Clickjacking
- Cookie Tampering
- Credit Card Theft
- Cross Site request forgery
- Cross site Scripting
- DoS
- HTTP Header Overflow
- Local File Inclusion
- Malicious Robots

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

- Man in the Middle
- Remote File Inclusion
- Server information leakage
- SQL Injection
- Malformet XML

Esta funcionalidad deberá contar con la posibilidad de escanear y analizar las aplicaciones web protegidas. Permitiendo identificar riesgos de seguridad y vulnerabilidades potenciales de estas aplicaciones.

Debe ser posible escanear parámetros en la URL para paquetes http tipo Get, para request http tipo POST y XML en el cuerpo del requerimiento http.

- HTTP GET
- HTTP POST
- XML en el Cuerpo del tráfico http
- AMF3 usado por Adobe Flash.

Deberá prevenir contra ataques de día cero por medio de:

- Validación de parámetros
- Manipulación de parámetros ocultos en la página.
- Especificar métodos aceptados http
- Constraint de http/HTTPS

- **Protección contra Web Defacement**

Esta característica deberá contar con la funcionalidad antidefacement la cual permita monitorear las aplicaciones, alertar y de ser necesario restaurar en caso de modificaciones no autorizadas de las aplicaciones web protegidas.

- **Análisis de vulnerabilidades**

Esta funcionalidad deberá realizar análisis de vulnerabilidades sobre las aplicaciones web protegidas, de tal forma que se identifiquen vulnerabilidades existentes en los aplicativos web del ICBF.

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

- **Protección DoS**

Esta funcionalidad deberá proteger contra ataques de denegación de servicio en http y https de tal forma que proteja a las aplicaciones web contra este tipo de ataques.

- **Autoaprendizaje de las aplicaciones web**

Esta funcionalidad deberá contar con la característica de autoaprendizaje de aplicaciones, la cual permita crear una línea base del comportamiento de la aplicación para creación de diferentes políticas de protección de aplicativos web.

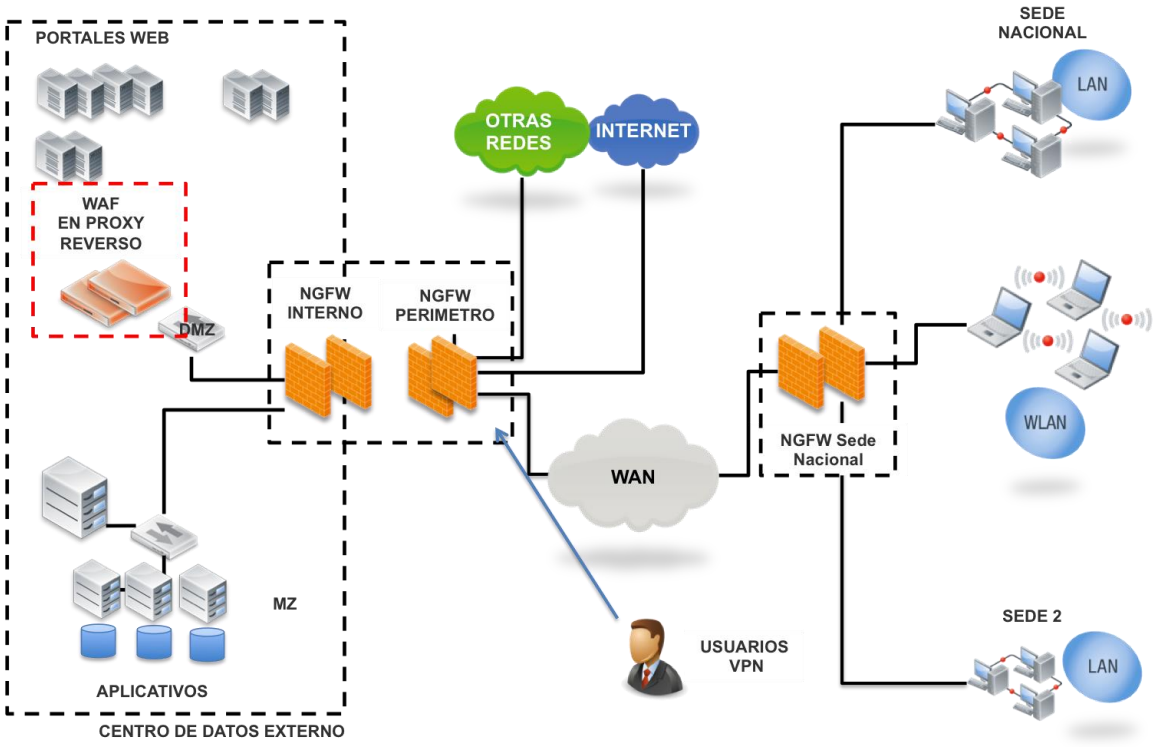
- **AntiMalware**

Esta funcionalidad deberá contar con un módulo de escaneo AntiMalware para hacer una revisión de los archivos que sean posteados o subidos a las aplicaciones web; evitando así que las aplicaciones sean atacadas con archivos infectados con malware.

- **Protección basada en Geolocalización**

Esta funcionalidad deberá contar con protección de ataques basados en la localización geográfica del atacante.

*** Arquitectura Mínima Requerida:**



6.3.6 Seguridad en Bases de Datos

EL CONTRATISTA durante la ejecución del contrato deberá suministrar, instalar, configurar, mantener, monitorear, y gestionar los Monitoreadores necesarios para la seguridad de las bases de datos del ICBF. La solución debe monitorear en tiempo real las actividades que se realicen sobre las bases de datos contando con las funcionalidades a continuación descritas.

El servicio de seguridad en bases de datos debe cumplir con los siguientes requerimientos mínimos:

* El servicio deberá estar arquitectado con Plataformas nuevas de Database Activity Monitoring, de propósito específico las cuales podrán estar en modo sniffer, sin embargo en caso de estar en modo in-line las plataformas deberán contar con alta disponibilidad, de tal forma que un fallo no genere indisponibilidad de las bases de datos que se están monitoreando. Por temas de desempeño, estas plataformas solo deberán tener este rol.

* El servicio deberá estar soportado con plataformas que cuenten con todas las interfaces de red necesarias para una óptima prestación del servicio.

* Los Motores a Soportar son:

- Oracle 10G R2
- Oracle 11.1.0.X
- Oracle 11G R2
- Microsoft SQL Server 2005 SP2
- Microsoft SQL Server 2008 SP2
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012

* Este servicio deberá contar con las siguientes características de seguridad:

- Módulo de DAM (Database Activity Monitoring)
- Módulo de Vulnerability Assessment
- Reportes

La Plataforma de Base de Datos debe cumplir con lo siguiente:

- La arquitectura de la solución debe soportar el monitoreo de al menos 160 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

- El monitoreo de base de datos preferiblemente debe hacerse por medio de puerto Mirror sin necesidad de agentes sobre la base de datos.

Cada una de las características de seguridad deberá permitir:

- **Módulo DAM (Database Activity Monitoring)**

El módulo DAM debe permitir centralizar el monitoreo y auditoria de la base de datos. Se deben mostrar alertas y reportes de estas alertas. Las alertas se deben poder configurar y deben ser de este tipo:

- Políticas de Metadata:
    - Para Oracle debe ser posible configurar Políticas de Packages, Synonyms, Tables, Tablespaces, Triggers, Views.
    - Para SQL Server debe ser posible configurar Políticas de Routines, Tables, Triggers, Views.
- Políticas de Privilegios:
    - Para Oracle debe ser posible configurar Políticas de Column Privilege, Profiles, Role Privileges, Roles, System Privileges, Table Privileges, User Privileges.
    - Para SQL Server debe ser posible configurar Políticas de Column Privileges, Member Privileges, Object Privileges, Roles, Server Roles, User Privileges.
- Políticas de Data de tipo Database, Table, Table and Column, Session y User.

Las Alertas generadas deben poder ser vistas en línea por el administrador, estas deben al menos mostrar la siguiente información:

- Nombre del Target (Host que tiene la instancia)
- Nombre de la Politica
- Reglas que fueron Violadas
- Severidad
- Acción
- Usuario

- Objeto usado
- Lugar (IP o Host)
- Hora

- **Módulo de Vulnerability Assessment**

La solución debe tener incluido un módulo de análisis de vulnerabilidades con las siguientes características:

- Debe ser capaz de realizar análisis de vulnerabilidades sobre motores de bases de datos por medio de la red, sin la instalación de un agente o alteración en la estructura de la instancia de base de datos.
- Las políticas de análisis de vulnerabilidades pueden ser personalizadas una a una y pueden ser usados en grupos.
- Los análisis de vulnerabilidades deben tener la capacidad de ser programados a criterios del administrador de la solución.
- Los análisis de vulnerabilidades deben reportar los hallazgos basados en los siguientes criterios : Severidad (Alto, medio, bajo e informativo) y Clasificación (Host, Base de Datos, Privilegios, Contraseñas, configuración e Informativo)
- Los análisis de vulnerabilidades relacionados con vulnerabilidades públicas, deben hacer referencia a bases de datos de públicas como lo son CVE u otras del mercado.
- Los análisis de vulnerabilidades deben reportar un resumen de los privilegios que se encuentran asignados en la instancia. Estos resúmenes deben proporcionar un listado completo de usuarios y roles descubiertos.
- La solución debe estar en la capacidad de descubrir de manera automática, los diferentes motores de bases de datos instalados en la red.

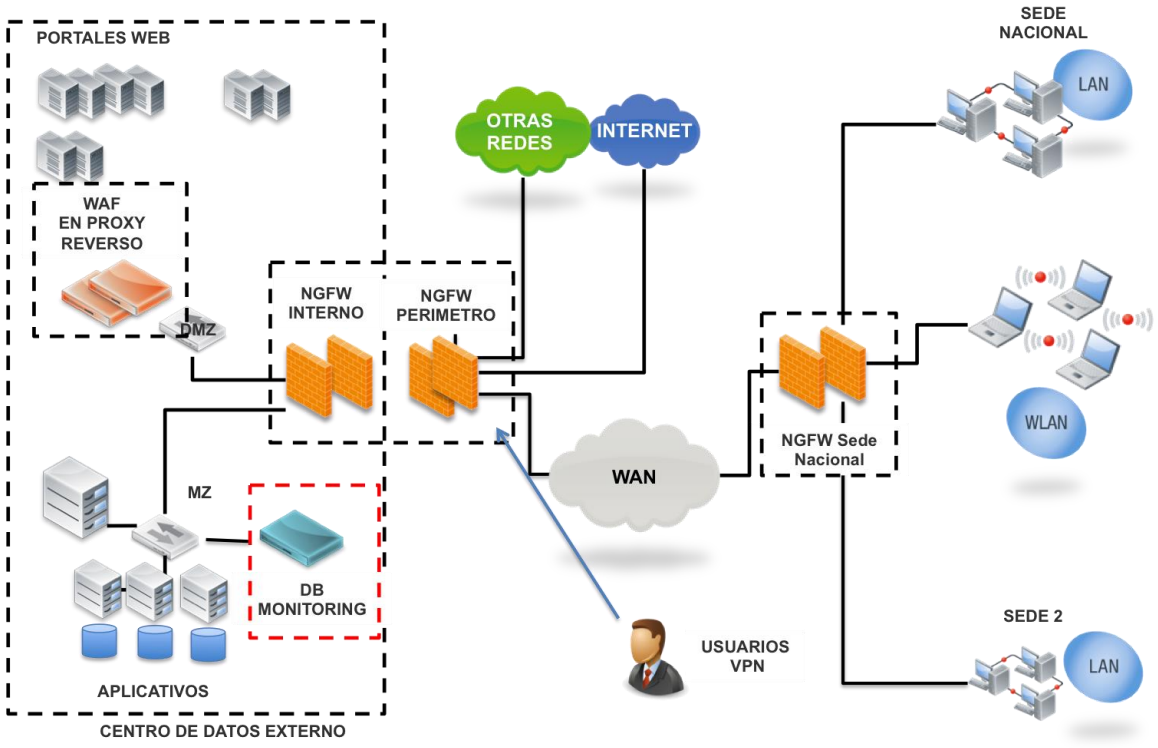
- **Reportes**

- La solución debe poder generar reportes predefinidos de fábrica de análisis de vulnerabilidades
- Debe poder generar reportes de Monitoreo y Auditoria predefinidos de fábrica.

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

- Debe poder generar reportes de Monitoreo y Auditoria personalizables por el administrador

*** Arquitectura Mínima Requerida:**



6.3.7 Logs y Reportes

El contratista deberá garantizar una funcionalidad/Plataforma que permite recibir Logs del firewall de nueva generación y el firewall de aplicaciones web, este dispositivo debe garantizar una retención de información de al menos 1 Año y debe ser posible generar reportes con esta información que le permita a la entidad tener visibilidad para poder tomar decisiones basado en esta información.

- Permite generar reportes personalizados, permite al administrador de la solución el determinar el contenido de los reportes.
- El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart)
- Genera reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.

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

- Genera reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.
- Genera reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.
- Permite generar reportes de la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino.
- Permite generar un reporte de las actividades administrativas (entradas de administradores, cambios de configuración) realizadas.
- Permite personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana.
- Permite especificar el período de tiempo específico para el cual el reporte va a ser obtenido, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año).
- Permite la calendarización de reportes.
- Tiene la opción de generar reportes en idioma inglés y en idioma español
- Permite enviar el reporte vía correo electrónico.

La solución debe incluir reportes predefinidos de al menos las siguientes categorías:

- Reporte de Eventos del sistema
- Aplicaciones usadas y Riesgos
- Aplicaciones y Consumos de anchos de Banda
- Aplicaciones y riesgo detallado
- Eventos de Seguridad y Análisis
- Reporte de Amenazas
- Seguridad y Análisis por usuario
- Uso Web

El módulo de Reportes y Logs debe incluir al menos:

- Capacidad de recibir hasta 250GB de Logs al día.
- Al menos 4 Interfaces RJ45 y 2 SFP.
- Debe soportar RAID 0, 1, 5, 6,10, 50, 60.
- 8 TB de Disco.

6.3.8 Servicio de Security Information Event Management (SIEM)

EL CONTRATISTA durante la ejecución del contrato proveerá, instalará, implementará, administrará, monitoreará y dará soporte del servicio de SIEM (Security Information Event Management) que cumpla con los siguientes requerimientos mínimos:

- ✓ Capacidad de agregación que permita la recolección de logs desde fuentes diversas incluyendo aplicaciones, bases de datos, servidores, equipos de usuario final, dispositivos de red y sistemas específicos para seguridad como firewall, IPS/IDS y antivirus, proporcionando la habilidad de consolidar los datos monitoreados de forma centralizada.
- ✓ Capacidad de búsqueda de atributos comunes para correlacionar los logs y eventos provenientes de diferentes fuentes y proporcionar información útil a partir de dicha correlación.
- ✓ Identificación de comportamientos anómalos basados en eventos y logs de múltiples tipos ocurriendo en un orden específico.
- ✓ Permitir la creación de reglas de correlación para la identificación de comportamientos anómalos o inesperados.
- ✓ Análisis automático y en tiempo real de eventos correlacionados y generación de alertas con notificación inmediata y codificada en colores a una consola de administración. También la posibilidad de alertar vía email.
- ✓ Consola de administración centralizada con las herramientas necesarias para presentar de forma gráfica la colección de logs, alertas y patrones de comportamiento en tiempo real, identificando y resaltando automáticamente aquellos que no se ajustan a los patrones normales.
- ✓ Retención de datos históricos que permitan la correlación de eventos a través del tiempo y el desarrollo de análisis forense.
- ✓ Habilidad de búsqueda en logs de diferentes nodos y periodos de tiempo basado en criterios de búsqueda específicos.
  Producción de reportes personalizables que se puedan adaptar a los procesos de auditoría y gestión de incidentes.

6.4 ALMACENAMIENTO

EL CONTRATISTA se encargara de la administración, operación, configuración y monitoreo de las soluciones de almacenamiento SAN y NAS con las que cuenta el ICBF, así como la gestión de nuevo software y hardware que adquiera el ICBF para el mejor desempeño del almacenamiento. Al igual que la implementación de las recomendaciones y solicitudes realizadas por parte de la entidad.

6.5 RESPALDOS (BACKUP)

EL CONTRATISTA se encargará de la administración, operación, configuración, y monitoreo de las soluciones de respaldo con las que cuenta el ICBF, al igual que la gestión sobre soluciones complementarias a las actualmente existentes, tales como

sistemas de backup en disco o soluciones de respaldo en la nube apropiando las recomendaciones y solicitudes recibidas por parte de la entidad.

En la actualidad el ICBF administra un promedio de 212 políticas de Backup vigentes, más las solicitudes de backup por demanda que mensualmente se requieran.

6.6 TELEFONIA IP

El CONTRATISTA debe prestar el servicio de administración de la plataforma de telefonía IP del ICBF a nivel nacional, esta se describe en el Anexo 001 – TABLAS LINEA BASE, garantizando al ICBF la continuidad del servicio, para ello EL CONTRATISTA deberá instalar y administrar en alta disponibilidad los servidores y equipos principales que componen la solución en el Data Center Externo ofrecido por EL CONTRATISTA.

Estas son las actividades mínimas que realizará EL CONTRATISTA durante la ejecución del contrato:

- Actividades que tengan como objetivo informar sobre el uso de terminales, servicios o aplicaciones de la plataforma.
- Atención de procedimientos internos del ICBF o ejecución de estos.
- Actualizaciones de Directorios o registros de usuarios en la plataforma.
- Configuraciones o programaciones de terminales.
- Configuraciones o programaciones de líneas externas.
- Revisión o solución de problemas de conectividad.
- Traslados de terminales, equipos Media Gateway o en su defecto sedes.
- Chequeo periódico de equipos de Red, equipos de telefonía o terminales telefónicas.
- Soporte a Ingenieros regionales, Ingenieros de Soporte o personal con labores de telefonía o labores de red.
- Seguimiento y monitoreo al desempeño de la plataforma.
- Mantenimiento de bases de datos.
- Actualizaciones registros de usuarios, memorias, códigos de cuenta, etc.
- Creación de terminales.
- Modificación de parámetros relacionados con terminales.
- Creación o modificación de datos relacionados con tratamiento de llamadas entrantes y salientes.
- Control a hardware instalado.
- Capacitaciones técnicas.

- Informes estadísticos y de operación.
- Coordinación de trámites de ingreso a las sedes del ICBF.
- Coordinación de actividades en todas las sedes del ICBF.
- Reporte de actividades en herramienta de gestión de mesa de servicio.
- Realización de tareas de Backup, respaldos de forma periódica de la planta telefónica.
- Configuración de equipos nuevos.
- Traslados de equipos de telefonía.
- Nuevas integraciones con la plataforma de telefonía IP.
- Solicitudes especiales de configuración como desarrollo de nuevos servicios o conexiones.

6.7 APLICACIONES

El CONTRATISTA, debe garantizar la administración, configuración, monitoreo y gestión de la disponibilidad, seguridad, seguimiento, control, continuidad, operación y buen desempeño de las aplicaciones con las que cuenta actualmente el ICBF y aquellas que surgieran durante la vigencia del contrato (Ver Anexo 001 - TABLA LINEAS BASE), realizar el despliegue, recomendaciones de mejores prácticas en configuración y puesta en producción de las aplicaciones que se requieran implementar durante la duración del contrato siguiendo para ello el procedimiento interno del ICBF para puesta en producción de proyectos de software. La infraestructura y licenciamiento serán provistos por el ICBF.

En caso de que se presenten fallas en el servicio, se deberá, a través de la estrategia de soporte planteada en la propuesta por EL CONTRATISTA, restablecer el acceso y disponibilidad de las aplicaciones del ICBF de acuerdo a los ANS establecidos en el menor tiempo posible.

Cumplir con tareas y tiempos establecidos y acordados en los planes de trabajo y los requeridos en la operación, para los proyectos que se presenten durante la vigencia del contrato.

6.8 BASES DE DATOS

El CONTRATISTA debe garantizar la administración, configuración, monitoreo y la gestión de la disponibilidad, seguridad, seguimiento, control, continuidad, operación y buen desempeño de la infraestructura de las bases de datos con las que cuenta actualmente el ICBF en los diferentes ambientes, así como aquellas que se adquieran durante la vigencia del contrato, que soportarán los sistemas de información del ICBF.

Servicio de administración y consultoría (asesoría) de Bases de Datos para todas las bases de datos que el ICBF utiliza. Igualmente incluye la administración y consultoría de las bases de datos en los diferentes ambientes que se alojen tanto en el Data Center Externo de EL CONTRATISTA, como en el Centro de Cómputo de la sede de la dirección general y las que adquiera durante la vigencia del contrato.

En caso de que se presenten fallas en el servicio, se deberá, a través de la estrategia de soporte planteada en la propuesta por EL CONTRATISTA, restablecer el acceso a las base de datos de acuerdo a los ANS establecidos en el menor tiempo posible.

Recibir, administrar y suministrar consultoría sobre bases de datos que se encuentran operando actualmente y las bases de datos nuevas que ingresarán en producción durante la vigencia del contrato, de acuerdo al procedimiento interno del ICBF de Puesta en Producción de proyectos de Software.

Proponer implementar y administrar esquemas de alta disponibilidad para las bases de datos actuales y para aquellas nuevas que surjan durante la vigencia del contrato y según la operación lo exija, utilizando el hardware que proporcione el ICBF (Servidores, SAN), o es su defecto como IaaS en caso de que el ICBF lo requiera. El ICBF proporcionará las licencias necesarias para los motores de bases de datos.

Realizar el montaje, administración, consultoría y soporte del motor de base de datos y de componentes tales como reporting services, integration services, analysis services, business Intelligence.

EL CONTRATISTA debe analizar, realizar y garantizar la correcta migración de las bases de datos ya sea de versión, edición u otro motor de base de datos, de acuerdo a los requerimientos del ICBF sin generar costo adicional al ICBF. Es responsabilidad de EL CONTRATISTA apoyar al ICBF en la validación de la compatibilidad de los aplicativos con las nuevas versiones de bases de datos.

Cumplir con tareas y tiempos establecidos y acordados en los planes de trabajo y los requeridos en la operación, para los proyectos que se presenten durante la vigencia del contrato.

6.9 OFFICE 365

EL CONTRATISTA debe garantizar la administración, configuración, operación y monitorear de la plataforma de **Office 365**, la cual estará conformada por los servicios e Infraestructura de:

- Servicios de Sincronización y Federación para Office 365
- Exchange Server 2013
- SharePoint Server 2013
- Lync Server 2013
- Exchange Online
- SharePoint Online
- Lync Online
- Yammer

Y realizar la gestión de soporte y técnica con fabricante, realizar el mantenimiento, migración, upgrate de la infraestructura, sus servicios, componentes y/o unidades lógicas en caso de ser requerido.

Office 365, cuenta con un servicio de conexión para teléfonos Blackberry (Plataforma BES) la cual forma parte del servicio de Office 365, EL CONTRATISTA debe administrar esta plataforma.

A continuación se amplía la información sobre los servicios de Office 365:

Servicios de Sincronización y Federación

Estos servicios están basados en Microsoft Forefront Identity Manager (FIM), y Microsoft Sync, para sincronización de directorio activo con Microsoft Azure, estos servicios están sobre una infraestructura de 3 Servidores que alojan los servicios que permiten iniciar sesión de forma federada con Office 365, y los servicios de sincronización que permiten activación de Licencias, Buzones, y premisos en Sharepoint Online.

Exchange Server On-premise

Este servicio está alojado de manera local en una infraestructura de 6 servidores, de acuerdo al documento de Línea Base, funciona bajo sistemas operativos Microsoft Windows Server y Microsoft Exchange Server 2010, y se tiene proyectada la migración a Microsoft Exchange Server 2013, la cual quedara realizada en la presente vigencia y con el Outsourcing actual, este servicio permite la gestión de correo electrónico en conjunto con Exchange Online, y aún se conserva esta infraestructura ya que actualmente no se tiene el 100% del personal de la entidad en la Nube, el flujo de correo hacia esta infraestructura viene directamente de Office 365 (nube) y es filtrado por el servicio EOP (Exchange Online Protection) indiferente si el buzón está alojado en la nube o en la infraestructura local.

SharePoint Server 2013

Actualmente este servicio funciona sobre una infraestructura de 3 Servidores locales basados en Microsoft Windows Server, este servicio no está integrado con Office 365 (Nube), se tiene proyectado para la conformación de algunos sitios bajo demanda, los

cuales deben ser administrados por EL CONTRATISTA, las bases de datos de este servicio deberán ser administradas, configuradas, monitoreadas y respaldadas.

Lync Server 2013

Actualmente este servicio funciona sobre una infraestructura de 3 Servidores locales basados en Microsoft Windows Server, este servicio está integrado con Office 365 (Nube) y los servicios de Directorio Activo Locales. Se debe garantizar la correcta operación de esta infraestructura 7x24 ya que de la misma depende el inicio de sesión tanto de usuario en Office 365 (nube) como usuarios en la infraestructura local. Este servicio también se encuentra integrado con la solución actual de videoconferencia de Polycom, la cual interactúa de forma nativa con Lync Server Local.

Exchange Online

Es el servicio que gestiona todo el correo electrónico en Office 365 (nube), el cual está configurado de forma hibrida con el servicio de Exchange Server On-premise, se manejan buzones de: usuario, compartidos y de recursos, adicionalmente los grupos de distribución están replicados con los del servicio On-premise.

Exchange Online tiene el servicio de EOP (Exchange Online Protection) que en conjunto con las reglas de flujo de correo garantizan la protección y filtrado de correo de toda la organización, solución que debe ser administrada por EL CONTRATISTA y basada en las directrices de seguridad que estipule el ICBF.

Para el backup de buzones el contratista debe usar las herramientas de retención y descarga que vienen incluidas con la plataforma de Office 365.

Sharepoint Online

Es el servicio donde se ubican actualmente 7 Sitios, pero se tiene proyectada la implementación en todas las Direcciones y SubDirecciones de Sede Nacional y Regionales. Cada sitio cuenta con permisos de acceso por usuario o por grupo, la implementación a Nivel Nacional se encuentra en fase inicial, pero EL CONTRATISTA debe administrar y apoyar técnicamente esta implementación que es totalmente Lógica ya que este es un producto que se tiene por servicio y por demanda. El ICBF contara con un administrador y líder global del proyecto, y definirá la estrategia de administración de toda la solución tanto On-Line como On-Premise.

Lync Online

Este servicio permite la conexión a LYNC de todos los usuarios que tienen licencia de Office 365 (Nube) activa, este servicio está configurado de forma hibrida con el servicio LYNC On-Premise, la administración de este servicio no tiene la misma complejidad del servicio LYNC

On-Premise ya que su funcionalidad está casi implícita en la administración global de Office 365.

Yammer

Este servicio permite la colaboración social en el ICBF, es un servicio totalmente de nube, y la administración está a cargo del ICBF mediante el administrador global y los Community Managers, este servicio esta federado para el inicio de sesión único mediante un servidor On-Premise que pertenece a los servicios de Federación de Office 365 para el ICBF, y el cual debe estar gestionado y administrado por EL CONTRATISTA.

6.10 HERRAMIENTAS DE GESTION Y MONITOREO

Actualmente el ICBF, cuenta las siguientes herramientas de Gestión y Monitoreo:

- Unisphere, Navisphere, Analyser EMC, Thin Provisioning EMC, SAN Copy EMC, SnapView EMC, Fast Suite EMC, la cual debe ser Gestionada, Administrada y Monitoreada por EL CONTRATISTA con personal certificado en la misma.

- Networker y Avamar para gestión de Backups, la cual debe ser Gestionada, Administrada y Monitoreada por EL CONTRATISTA con personal certificado en la misma.

- Microsoft System Center:

    - La solución está completamente licenciada para los siguientes módulos:
        - Configuration Manager + Endpoint Protection
        - Service Manager
        - Operation Manager
        - Virtual Machine Manager
        - Data Protection Manager
        - Orchestrator

    De los cuales se encuentran en operación actualmente, Configuration Manager + Enpoint Protection, Virtual Machine Manager, WSUS (Capitulo de Seguridad), KMS (Capitulo de Servidores) los cuales deben ser gestionados, administrados y monitoreados en todas sus funcionalidades y módulos por EL CONTRATISTA con personal idóneo para este fin.

EL CONTRATISTA deberá implementar y operar el módulo System Center Operations Manager para el monitoreo y control de la infraestructura el ICBF.

EL CONTRATISTA deberá usar la Suite System Center para cumplir los requerimientos del presente documento a nivel de herramientas, en caso de necesitar algún módulo de System Center no implementado, EL CONTRATISTA podrá implementar y operar el mismo el pro del beneficio y utilización de herramientas propias del ICBF.

La implementación parcial o total de la Suite System Center por parte del CONTRATISTA será total propiedad del ICBF sin que ello represente costos adicionales para el ICBF.

En caso de que la Suite System Center o las herramientas antes expuestas no cumplan algún requerimiento del presente capitulo, EL CONTRATISTA deberá suministrar las herramientas adicionales que considere necesario para el cumplimiento del presente previo concepto-consulta técnica del fabricante de las herramientas que están como propiedad del ICBF donde se evidencie el no cumplimiento del requerimiento específico.

El ICBF proveerá la infraestructura para las herramientas que sean de su propiedad (ICBF) que estén implementadas o que estén por implementar.

El ICBF no proveerá la infraestructura para las herramientas de propiedad del Contratista o que sean suministradas durante la ejecución del contrato y las mismas deberán estar alojadas en la infraestructura del contratista.

EL CONTRATISTA deberá integrar las herramientas del ICBF y las que suministre EL CONTRATISTA con la aplicación de Mesa de Servicio, de acuerdo a la herramienta que el proveedor de ese contrato suministre.

Si el contratista llegase a suministrar una o varias herramientas para cumplimiento del presente contrato, las mismas deben ser de dedicación exclusiva del ICBF y no compartidas con otros proyectos.

De acuerdo a lo anterior EL CONTRATISTA deberá:

1. Mantener, Administrar y Operar las herramientas que están actualmente implementadas en el ICBF.
2. Implementar, Administrar, Mantener y Operar System Center Operations Manager.
3. Suministrar Herramienta (s) en caso de que las herramientas del ICBF de forma comprobada técnicamente no cumplan algún requerimiento que se solicite.

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

4. Integrar las Herramientas del ICBF y EL CONTRATISTA con la aplicación de Mesa de Servicio.

Las herramientas propiedad del ICBF y/o suministradas por EL CONTRATISTA destinadas para el ejercicio de Administración, Mantenimiento y Operación de la Infraestructura deberán permitir y/o hacer:

- Ejecución de acciones de notificación automáticas e inmediatas ante la aparición de condiciones de anormalidad que afecten la prestación del servicio
- Acceso remoto que permita configurar, administrar, obtener estatus del monitoreo en tiempo real y generar reportes
- Autenticación segura incluyendo cifrado de contraseñas para acceso a los sistemas.
- Capacidad de integrarse al directorio activo para controlar el acceso a la herramienta.
- Debe estar alineada a los procesos y procedimientos de ITIL de acuerdo a las buenas prácticas de la Industria.
- Debe permitir la creación automática de tickets en la Mesa de Servicios ante la generación de eventos.
- Debe permitir la generación de reportes de auditoría a través de la consola de administración que debe ser suministrada al ICBF de acuerdo con los perfiles definidos por la Dirección de Información y Tecnología para llevar a cabo el seguimiento y control.

Para el ICBF se interpreta como Puntos Finales (END POINTS), todos los equipos y/o dispositivos que tengan conexión a la Red, como lo pueden ser Computadores, Servidores, Dispositivos móviles, equipos de red, servidores (físicos y virtuales), Impresoras, Aires Acondicionados (que posean conectividad de red), UPS (con conectividad de Red) entre otros, que sean propiedad o que estén al servicio del ICBF.

- Permitir la distribución de software de manera automatizada a toda la plataforma tecnológica de la red del ICBF (End Points).
- Permitir la gestión y el monitoreo de los Puntos Finales del ICBF.
    - Computadores PC, Portátiles y Tablets
    - Dispositivos Móviles.
    - Equipos de Red.
    - Servidores.
    - Impresoras
    - Escaneres
    - Aires Acondicionados (que posean conectividad de red)
    - UPS (conectividad de red)
- Permitir controlar la línea Base de Software para la Infraestructura del ICBF.
- Desplegar Actualizaciones masivas o direccionada de Software.

- La herramienta debe permitir crear y distribuir por red imágenes de sistemas operativos de forma centralizada de acuerdo a cada referencia o característica de equipo. Debe también permitir la preparación y alistamiento masivo de máquinas.

Administración de licenciamiento

EL CONTRATISTA debe Monitorear y Administrar el Licenciamiento del ICBF a través de las Herramientas que el ICBF disponga para este fin, como lo es el caso de KMS Server, y las que el ICBF adquiera para este fin durante el transcurso del Contrato.

- **APLICACIONES**

  - Monitorear las transacciones de las aplicaciones e identificar rápidamente los cuellos de botella en dichas aplicaciones.
  - Monitorear las transacciones de usuario y carga efectuada en servidor, base de datos y back-end.
  - Identificar componentes afectados por degradación del servicio.
  - Proporcionar alertas eficientes y en tiempo real para los problemas de rendimiento de aplicaciones y disponibilidad.
  - Rastreo y seguimiento de transacciones para identificar posibles cuellos de botella.
  - Contadores de rendimiento de servicio Web IIS donde se proporcione:
    - Bytes enviados por segundo
    - Bytes recibidos por segundo
    - Recibe peticiones por segundo
    - Publica solicitudes por segundo
    - Máximo de conexiones
    - Not Found (404) Error por segundo
    - Porcentaje de tiempo de procesador
    - Caché Porcentaje Hit
    - Solicitar Tiempo de espera
    - Transacciones por segundo

  Además de todas las métricas que EL CONTRATISTA y/o el ICBF requiera para garantizar el óptimo funcionamiento de las aplicaciones.

- **BASE DE DATOS**

  Oracle:

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

- Mensajes de alerta de log de Oracle para corrupciones de bloques de datos, colas de recursos excedidos, errores internos y fallas de lectura/escritura de I/O
- Situaciones de error como estado SYS.DUAL
- Monitoreo de los principales proceso de Oracle: LGWR, DBWR, PMON, ARCH, SMON, TRWR, RECO, SNPx y LCKx
- Deberá monitorear variables de desempeño propias del manejador de bases de datos Oracle
- Deberá permitir el monitoreo de las principales variables de manejo de espacio de Oracle, tales como: table spaces, espacio libre y fragmentación de segmentos
- Deberá permitir el monitoreo de variables del desempeño del manejador tales como: Sort, buffer, shared pool, dictionary cache ratio, etc.
- Deberá manejar estadísticas de los segmentos de Rollback, tales como: número de shrinks, porcentaje de esperas
- Deberá manejar información de Archive, tal como: tiempo promedio entre escrituras de archive log y numero de logs que caben en un dispositivo archive.
- La solución de administración de Oracle deberá soportar las versiones 7, 10g y superiores de Oracle.
- Validación de configuraciones de Oracle a nivel de Monitoreo.
    - Gestión de disponibilidad y rendimiento de Oracle.
    - Monitoreo del archivo Alert.log (validar y verificar errores).
    - Monitoreo de estadísticas de rendimiento, tales: como actividad del usuario, el estado, espacio, rendimiento del SGA, detalles del SGA, estado del SGA, detalles de las sesiones, tablas de uso de espacio, detalles del espacio, alarmas, comportamiento de los archivos de datos, Obtención del buffer, lectura en disco, segmentos del roollback, consultas, entre otras.
    - Monitoreo de backups, (modo: archive), y/o Exports; según la metodología implementada.
    - Planes de mantenimiento y optimización.
    - Monitoreo de seguridad.
    - Monitoreo de Tablespace.

Microsoft SQL Server:

- Personalizar métricas y alarmas integradas SQL Server
- Automatizar análisis de métrica de rendimiento del motor SQl Server
- Posibilidad de supervisar y controlar las base de datos SQL Server en cualquier momento desde cualquier dispositivo.
- Generar alertas instantáneas a nivel de servidor y determinar la causa raíz de posibles problemas en Base de datos SQL Server

- Capacidad de diagnosticar y resolver problemas de forma proactiva y precisa, antes de que afecten disponibilidad o rendimiento de aplicaciones del ICBF.
- Detectar y diagnosticar problemas de rendimiento.
- Identificar rápidamente los servidores donde se origina la degradación del rendimiento y aislar la causa raíz de un problema de rendimiento para agilizar el diagnóstico y resolución de problemas.
- Tuning automatizado para SQL Server
- Diagnósticos profundos físicos, de cloud y virtuales de SQL.
- Identificar sentencias costosas T-SQL con base en la utilización de índices, consumo de recursos de hardware o eficiencia de las consultas.
- Proporcionar información detallada de las actividades y entornos de los clústers, duplicación, replicación de bases de datos y actividades de log-shipping y entornos de SQL Server.
- Tendencias de capacidad, actividad y performance de motores de base de datos SQL Server.
- Identificar consultas costosas.
- Capacidad de almacenamiento de datos métricos a largo plazo para obtener tendencias históricas e iniciativas de planificación de la capacidad.
- Diagnosticar y determinar origen de las esperas y cuál es la causa.
- Detección y revisión de bloqueo.
- Capacidad de controlar fragmentación de índices
- Medición de Longitud de Cola.

MySQL:

- Generación de alarmas cuando se superen los umbrales normales de operación para:

  - Información de cache (cache hit percentage, cache free buffer percentage)
  - Utilización de CPU por MySQL
  - Requerimientos de escritura de la base de datos a sistema operativo que no han sido completados
  - Espacio del log de transacciones usado por cada base de datos

- Deberá colectar información histórica de rendimiento para las siguientes métricas:

  - Uso de CPU por sesión
  - Buffers scanned

- Deadlocks
- Timeouts
- Enqueue Waits
- Free buffer inspected
- Free buffer requested
- Active_sorts

- Debe ofrecer reportes y gráficas de desempeño de las métricas colectadas.

- **SERVIDORES**

- Permitir el monitoreo de los componentes de la infraestructura que soportan los servicios, incluidos servidores tanto físicos como virtuales.
- Monitorear servicios de red como: DHCP, DNS, FTP, ping, port monitor, SNMP, Trap, y MIB
- Configuración de alarmas con niveles de criticidad personalizables y asociables a variables de monitoreo.
- Presentar a través de sus consolas en forma consolidada las alarmas generadas por los nodos, tener capacidades de filtrado y reflejar gráficamente el estado de cada nodo monitoreado.
- Asociar políticas de monitoreo a servidores o grupo de servidores.
- Tener alcance sobre máquinas con sistemas operativos Microsoft y Linux como mínimo
- Monitorear y procesar en tiempo real y durante toda la ejecución del contrato como mínimo el estado de las siguientes variables:
  Windows/% Total proccesor time
  Windows/Processor queue length
  Windows/Carga de transacciones
  Windows/Disk time
  Windows/Disk queue lenght
  Windows/Page Fault/sec
  Windows/Pages/sec
  Windows/Pool Nonpaged bytes
  Windows/Paginación
  Windows/Procesos de S.O. críticos (Lsass, Svchost, Ntfrs)
  Windows/Servicios de S.O.
  Windows/Servicios de Directorio Activo
  Linux/Utilización de CPU
  Errores de disco
  File Systems
  Utilización de Memoria
  Procesos
  Mensajes y actividades de semáforos

- Monitorear el uso de recursos lógicos de servidores y 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

6.11 GOBERNABILIDAD

6.11.1 ORGANIZACIÓN DEL PROYECTO

EL CONTRATISTA deberá desarrollar los planes para la gerencia del proyecto, proveer el personal requerido, participar en comités definidos con el fin de garantizar la adecuada ejecución y cumplimiento del contrato, para efectos de aplicar las mejores prácticas de gobierno de tecnología. A continuación se mencionan los Stakeholders relacionados en el proyecto:

ICBF: Instituto Colombiano de Bienestar Familiar: Es el contratante de servicios de infraestructura, valor agregado y conexo bajo la modalidad de Outsourcing.

EL CONTRATISTA: Es el responsable de la ejecución del contrato de acuerdo con los documentos que lo soportan. Así mismo, EL CONTRATISTA debe cumplir con los criterios de ANS establecidos de tal forma que proporcione un excelente servicio para los usuarios del ICBF, debe garantizar la instalación, administración, operación, mantenimiento y soporte de toda la plataforma tecnológica del ICBF, tanto propia como arrendada.

ASEGURAMIENTO DE CALIDAD: Es el responsable de la definición y aplicación de métodos de verificación y control de calidad de los servicios contratados a través de la verificación, realización y control de mediciones y la realización de estudios de apreciación, percepción y valoración del servicio por parte de los usuarios del ICBF.

6.11.2 ROLES

La organización del proyecto estará conformada por cargos que permitirán dirigir y coordinar la labor realizada por el personal involucrado en el proyecto, con el propósito de mantener el buen desarrollo de las actividades del mismo.

A continuación se describe cada uno de los roles dentro del proyecto:

Supervisión del contrato: El ICBF controlará el cumplimiento de las obligaciones por parte de EL CONTRATISTA a través del Director de Información y Tecnología o a quien este delegue. Este rol ejercerá la supervisión del presente contrato conforme a lo dispuesto sobre el particular en las normas internas expedidas para el efecto por el ICBF. Es además el encargado de la dirección, control y seguimiento del desarrollo del proyecto. Ejercerá sus actividades a través de tres roles:

- Grupo de Verificación y Control.
- Gerencia del proyecto.
- Grupo de Medición y Seguimiento.

Gerente del Proyecto ICBF: Responsable del proyecto al interior del ICBF. Su función es interactuar con EL CONTRATISTA y coordinar el equipo de trabajo y las actividades al interior del ICBF. Esta actividad será realizada por el Subdirector de Recursos Tecnológicos o por la persona a quien él designe para ello.

Grupo de Medición y Seguimiento: Este grupo será el encargado de realizar las labores de medición y seguimiento a los ANS de este contrato y estará conformado por los especialistas líderes de cada servicio, tanto del ICBF como de EL CONTRATISTA.

Grupo de Verificación y Control: Este grupo o el funcionario del ICBF encargado de realizar las labores de supervisión Administrativa, legal y financiera al contrato.

Gerente del Proyecto CONTRATISTA: Responsable del proyecto por parte de EL CONTRATISTA. Su función es dirigir y coordinar a su equipo de trabajo con el propósito de cumplir con los criterios definidos para cada uno de los servicios, proponer sus puntos de vista en reuniones programadas, teniendo en cuenta los diferentes escenarios y casos presentados en el transcurso del desarrollo del proyecto.

EL CONTRATISTA de Mesa De Servicio: Es el responsable de la ejecución del contrato de Mesa de Servicio suscrito con el ICBF y en el cual existen servicios que se interrelaciona con el presente contrato, tales como: Control y gestión de las solicitudes relacionadas con conectividad de las redes.

EL CONTRATISTA de Redes: Es el responsable de la ejecución del contrato de Redes suscrito con el ICBF y en el cual existen servicios que se interrelaciona con el presente contrato, tales como la red de área amplia (wan), red de área local (lan), red inalámbrica (wlan), internet e internet móvil del ICBF.

ITIL: Durante el tiempo de duración del contrato, EL CONTRATISTA deberá asignar un responsable que asuma el rol para cada proceso ITIL solicitado en este documento por el ICBF.

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 roles para cada proceso de ITIL descrito a continuación se requieren con dedicación exclusiva y deberán contar con el conocimiento y experiencia en ITIL v.3 o superior.

No deben existir más de dos roles ITIL asignados a una sola persona.

Dichos roles son:

- Gestor de Cambios.
- Gestor de Incidentes.
- Gestor de Problemas.
- Gestor de Capacidad.
- Gestor de Niveles de Servicio.
- Gestor de Continuidad.
- Gestor de Disponibilidad.
- Gestor de Riesgos.

Nota: EL CONTRATISTA deberá permanecer en constante comunicación con los dos proveedores de servicios adicionales (Redes y Mesa de Servicios) con el fin de garantizar el buen funcionamiento tecnológico del ICBF. Con el objeto de oficializar los temas que requieren de la integración, estos se harán a través de un Comité de Interlocución y se deben dejar previamente plasmados en el plan de interlocución el cual es elaborado por los tres contratistas.

Debe cumplir con los criterios de ANS establecidos de tal forma que proporcione un excelente servicio para los usuarios del ICBF, debe garantizar la instalación, administración, operación, mantenimiento y soporte de toda la plataforma tecnológica del ICBF, tanto propia como arrendada, descrita en este documento.

6.11.3 Comités

Adicionalmente se conformarán comités, en los cuales se realiza seguimiento sobre la evolución y resultado del proyecto, entre ellos se encuentran:

- Comité Ejecutivo
- Comité Operativo
- Mesas de trabajo por líneas de servicio
- Comité de interacción entre los proveedores de Infraestructura, Mesa de Servicio, Redes e ICBF.

Los integrantes de los comités se definirán en los primeros 15 días de la etapa de transición entrada.

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

A las reuniones de trabajo es posible que se inviten a participar a funcionarios del ICBF o de EL CONTRATISTA cuando las condiciones así lo requieran, en estos casos, la participación de dichas personas será programada a través del Gerente del Proyecto ICBF o por la persona a quien él designe para ello.

Comité Ejecutivo: Mensualmente o de acuerdo a la necesidad del ICBF, se reunirán los representantes gerenciales del ICBF, para hacer seguimiento en temas administrativos, y financieros y revisar los escalamientos del comité operativo. Estará conformado por el Supervisor del contrato, el Gerente del Proyecto del ICBF y el Gerente de El CONTRATISTA.

Comité Operativo: Periódicamente y según la necesidad el ICBF o cuando se considere conveniente, se realizará el seguimiento a la prestación del servicio y las tareas y proyectos acordados entre ambas partes. También será el espacio para tratar aspectos especiales que no se hayan resuelto en las Mesas de trabajo de cada servicio. A este comité asistirá el líder del servicio por parte del ICBF y el gerente del proyecto por parte de EL CONTRATISTA y en caso de ser requerido se convocarán otros miembros de cada equipo de trabajo.

Mesas de trabajo por Líneas de servicio: El líder del servicio tanto del ICBF como los coordinadores de cada servicio de EL CONTRATISTA cuyos perfiles están definidos en el Anexo 006 - PERFILES-PROFESIONALES REQUERIDOS. Deben estar en continua comunicación con el objeto de mantener el control del funcionamiento de cada servicio, para ello se reunirán mínimo dos (2) veces por mes o de acuerdo a la necesidad del ICBF, con el objeto de validar el informe de gestión mensual presentado por EL CONTRATISTA, hacer seguimiento a las actividades y satisfacer las necesidades del ICBF referentes a cada uno de los servicios. A las mismas deberán asistir los miembros del equipo de trabajo de EL CONTRATISTA, requeridos según el tema a tratar en cada una de ellas. Los coordinadores del equipo de trabajo del EL CONTRATISTA, deberán asistir a las mesas de acuerdo a su responsabilidad en cada tema. La citación a dichas mesas, será realizada por el líder de servicio del ICBF en el momento requerido. De estas reuniones debe surgir un entregable que contenga aceptación del informe de gestión mensual. Los avances realizados, las actividades programadas con sus fechas de entrega, responsables y recursos el cual debe ser reportado a los gerentes del ICBF y de EL CONTRATISTA.

Comité de Interacción: Este comité lo conforman los Gerentes y/o Coordinadores de los Proyectos y Líderes de Grupo que se reunirán mensualmente o de acuerdo a la necesidad del ICBF y es liderado por el Gerente del ICBF o a quien el ICBF designe, para interactuar en los puntos en que convergen los servicios de todos los Contratistas de TIC que hacen parte del ICBF, deben generar los lineamentos, políticas, procedimientos que se

aplicarán a fin de solucionar los diferentes obstáculos que se presenten en el desarrollo de los contratos, también será el espacio para tratar aspectos especiales que no se hayan resuelto en las Mesas de trabajo de cada servicio y que estén relacionadas con los contratos de **REDES – INFRAESTRUCTURA – MESA DE SERVICIO**, este comité generara compromiso que serán de obligatorio cumplimiento para todos los contratos previa aprobación del Supervisor.

6.11.4 Planes requeridos durante la ejecución del contrato

Con el fin de realizar una gerencia adecuada al proyecto, EL CONTRATISTA deberá presentar un Plan de Proyecto global de acuerdo a las mejores prácticas de PMI, que permita conocer la ejecución de trabajos, actualizar las estrategias, realizar control sobre los entregables, servicios y procesos, así como planes para el diseño e implementación. Este debe permanecer actualizado durante toda la vigencia del contrato y debe contener como mínimo:

- ✓ Plan de trabajo: Cronograma y plan de control de las actividades, tiempos, responsables, ruta crítica y paquetes de trabajo.
- ✓ Plan de mitigación de riesgos del proyecto: Debe incluir la evaluación de riesgos, identificación de disparadores de riesgos, sus correspondientes planes de mitigación, remediación y planes de contingencia a los riesgos. Su seguimiento se realizará con presentación en el comité operativo y evaluación en el ejecutivo.
- ✓ Plan de calidad del proyecto: Debe incluir la definición clara, precisa y concertada de los procesos de aseguramiento y control de calidad de los diferentes entregables. Así como la definición de pruebas, procedimientos de aceptación y proceso de cierre del proyecto. En este plan se definen los criterios mínimos bajo los cuales el supervisor y la interventoría darán por aceptados los resultados del proyecto.
- ✓ Plan de comunicaciones del proyecto: Debe incluir canales, mecanismos y herramientas de comunicación con los diferentes Stakeholders. (Formatos de reportes, formatos de documentos, matriz de comunicaciones, agenda de reuniones, periodicidad de los informes, reuniones, reportes de avance).

  Este plan debe ser actualizado y divulgado a todos los Stakeholders. El ANEXO 007 - REPORTES DE OPERACIÓN, presenta de manera general los reportes mínimos que deben hacer parte del Informe general de estado, así como los reportes de operación mínimos, periódicos y no periódicos, que serán responsabilidad de EL CONTRATISTA.

  EL CONTRATISTA deberá generar los reportes que requiera el ICBF basados en las herramientas usadas por EL CONTRATISTA, adecuando la personalización y parametrización de los mismos de común acuerdo entre el ICBF y EL CONTRATISTA.

- ✓ Plan de recursos humano del proyecto: Definición de roles y responsabilidades del equipo del proyecto, fechas de entrada y salida de los integrantes del equipo. Los comités pertinentes, incluido el comité de control de cambios del proyecto (este comité es diferente al comité de cambios del servicio definido de acuerdo a ITIL.
- ✓ Plan de mejoramiento continuo sobre los servicios: EL CONTRATISTA debe establecer a este proyecto un proceso de mejoramiento continuo, para eso debe realizar seguimiento bimensual a las acciones de mejora y verificar la efectividad e impacto de las mismas. El modelo de servicio deberá brindar atención a las quejas, reclamos o sugerencias sobre el servicio prestado, así como obtener la percepción de los usuarios, a través de encuestas, estudios, estadísticas o cualquier otro esquema que permita evaluar el nivel de satisfacción sobre el proyecto.
- ✓ Procedimientos de control de cambio del proyecto y sistema de autorización de cambios.
- ✓ Plan de interlocución: Los contratistas tanto de INFRAESTRUCTURA, REDES y MESA DE SERVICIO deberán elaborar un plan en el cual se determine las actividades y los parámetros de control en que los Stakeholders deben interactuar para un efectivo cumplimiento de ANS y lograr la continuidad de los servicios con el propósito de que el ICBF brinde efectividad y eficiencia en la prestación de los servicios a sus beneficiarios, este plan debe ser aprobado por el ICBF.

6.11.5 Capacitación Equipo De Trabajo

Con el objeto de garantizar la correcta interacción entre el equipo de trabajo dispuesto por el ICBF para el seguimiento del proyecto, con el equipo técnico y líder, dispuesto por EL CONTRATISTA, éste último debe proporcionar los siguientes cursos técnicos y de gestión**, garantizando que sean la última versión disponible:**

NOMBRE DEL CURSO/CERTIFICACIÓN	DESCRIPCIÓN	No. DE CUPOS POR CURSO
ITIL	**Information Technology Infraestructure Library (Foundation)**	9
COBIT	**Control Objectives for Information and related Technology**	9
	Managing Office 365 Identities and Requirements	3

NOMBRE DEL CURSO/CERTIFICACIÓN	DESCRIPCIÓN	No. DE CUPOS POR CURSO
Office 365	**Enabling Office 365 Services**	
System Center	**Administering and Deploying System Center 2012 Configuration Manager**	3

El ICBF designará el personal que tomará los cursos y capacitaciones, entre quienes realizan el trabajo permanente de Atención y Servicio de la Subdirección de Recursos Tecnológicos, y definirá en coordinación con EL CONTRATISTA, el cronograma para su realización.

EL CONTRATISTA proporcionará al equipo de trabajo designado por el ICBF, los cursos y/o capacitaciones relacionadas en el cuadro anterior con los requisitos y certificaciones solicitadas por el ICBF de acuerdo al cronograma definido.

EL CONTRATISTA, deberá garantizar que todos los cursos serán realizados en las últimas versiones disponibles por el fabricante, deberán ser dictados por centros autorizados por el fabricante o entidad certificadora y deben incluir los exámenes de certificación oficiales del fabricante o certificador, teniendo en cuenta los costos que generen dichas certificaciones.

Esta capacitación se debe realizar una única vez, durante los 14 primeros meses de ejecución del proyecto, previa solicitud y cronograma presentado por el ICBF.

Las capacitaciones requeridas buscan afianzar algunas capacitaciones realizadas por el ICBF en otros proyectos y de esta manera fortalecer el conocimiento técnico y de gerencia de proyectos, indispensable para garantizar el adecuado seguimiento y gestión durante la ejecución del proyecto, garantizando así la adecuación y operación de los servicios.

7 OBLIGACIONES DEL CONTRATISTA

7.1 Obligaciones Específicas

Centro de Cómputo

Administración del Centro de Cómputo

1. Mantener los procedimientos de administración del Centro de Cómputo de la SEDE DE LA DIRECCIÓN GENERAL, documentados, actualizados y llevar el registro de fallas,

problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones, trabajos realizados y en general todos los detalles de la operación en una bitácora electrónica y en la CMDB administrada por EL CONTRATISTA designado por el ICBF, desde el inicio del contrato con los insumos de información provistos por el ICBF y a partir del descubrimiento automático o manual de inventario de la herramienta de gestión y monitoreo provista por el ICBF. EL CONTRATISTA deberá entregar información actualizada de los equipos para la alimentación de la CMDB al ICBF cuando este la requiera, Esta plataforma será administrada por el contratista de Mesa de Servicios.

2. Monitorear las condiciones ambientales del Centro de Cómputo, así como toda la infraestructura.

3. Controlar, custodiar y mantener los inventarios de los suministros y consumibles requeridos para una correcta operación del Centro de Cómputo de la sede de la dirección general, asegurando niveles adecuados de existencia y servicio, y mantener un registro actualizado de su utilización.

4. Diseñar, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de Centro de Cómputo de la sede de la dirección general.

5. Realizar el mantenimiento preventivo y/o correctivo incluyendo partes y/o repuestos dentro de los tiempos previstos a los proveedores del mantenimiento y/o soporte, cuando se presenten interrupciones en el servicio, averías o se ubiquen posibles fallas que puedan afectar el servicio de la infraestructura para el Centro de Cómputo de la sede de la dirección general.

6. Administrar y monitorear 7x24 la operación de la infraestructura del Centro de Cómputo de la Sede de la Dirección General.

7. Gestionar las condiciones ambientales y técnicas necesarias para el funcionamiento adecuado del CENTRO DE CÓMPUTO de la SEDE DE LA DIRECCIÓN GENERAL entregadas por el ICBF, en caso de daño en algún componente este deberá arreglador o reemplazado en forma inmediata por EL CONTRATISTA, con el fin de normalizar la operación. La temperatura adecuada que se debe mantener para los dispositivos informáticos deberá oscilar entre 18º y 25º C (64,5º y 77º F), con una humedad relativa de entre 40 y 55%.

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

8. Acompañar al personal técnico que adelante trabajos en el Centro de Cómputo del ICBF durante el desarrollo de su labor, previa comunicación del ICBF al EL CONTRATISTA sobre las actividades a desarrollar y los tiempos asociados por medio de la mesa de servicios.

9. Mantener el Centro de Cómputo de la SEDE DE LA DIRECCIÓN GENERAL, organizado, libre de obstrucciones.

10. Mantener informado al líder del servicio del ICBF sobre el funcionamiento del Centro de Cómputo de la SEDE DE LA DIRECCIÓN GENERAL.

11. Garantizar la gestión, administración y monitoreo para el correcto funcionamiento de los sistemas que componen el Centro de Cómputo tales como:
    - Aires acondicionados.
    - Sistema de puesta a tierra.
    - Identificación de todos los equipos y componentes de acuerdo a normatividad TIA 606.
    - Sistema de detección de incendios.
    - Sistema eléctrico regulado, soportado por UPS.
    - Control de seguridad física (seguridad perimetral, sistemas de vigilancia, sistemas de control de accesos).
    - CCTV.

    Nota: El ICBF entregará a EL CONTRATISTA los elementos mencionados con su respectivo inventario.

12. Realizar mantenimiento preventivo y/o correctivo incluyendo partes y/o repuestos de los siguientes equipos que se encuentran en el centro de cómputo de la sede de Dirección General:
    - Sistema Control de Incendios Fenwal M-2320 con agente FM200.
    - Transformador de aislamiento C&CO Energy Serie 1653-0 de 45 Kva, año de fabricación 2006, peso 250 kl.
    - Aires Acondicionados marca CATALAN modelo series 6
    - UPS de 30 kva marca APC
    - Control de acceso biométrico
    - Sistema eléctrico regulado y no regulado incluyendo todos sus componentes.
13. Mantener actualizada la información de los elementos que componen el Centro de Cómputo de la SEDE DE LA DIRECCIÓN GENERAL, los cuales incluyen entre otros:
    - Mapas e inventario de racks y/o equipos al servicio de ICBF alojados en ellos.

- Mapas distribución sistema contra incendio.
- Diagramas unifilares de tableros, puesta a tierra y sistemas eléctricos.
- Inventario de equipos con marca, modelo y referencia, incluyendo:
- Sistema contra incendio.
- Aires acondicionados y climatización.
- Trasformador de aislamiento
- Gestión de alarmas.
- Control de seguridad (seguridad perimetral, sistemas de vigilancia, sistemas de control de accesos).
- Topología del Data Center Externo y Centro de Cómputo

14. Socializar el procedimiento para el ingreso y salida de equipos del centro de cómputo del ICBF así como los formatos que se utilizarán para este fin.

15. Implementar los niveles de seguridad física necesarios para proteger todos los equipos que se encuentran en el centro de cómputo de la sede de Dirección General. Estas medidas de seguridad también aplican en el evento que el ICBF incorporen nuevos equipos propiedad de la entidad o equipos de terceros para proyectos o pilotos, éstos se reportarán con debida antelación a EL CONTRATISTA para que sean incorporados en su esquema de seguridad.

16. El ICBF requiere en cuanto a seguridad física, que EL CONTRATISTA implemente como mínimo controles físicos de registro de ingreso de personal autorizado tales como:

    Cámaras de video tipo **domo con infrarrojo**.Para el **centro de cómputo** se requieren seis (6) cámaras así: una (1) instalada en cada pasillo (para un total de 4 pasillos), una (1) visualizando la puerta de acceso y una (1) visualizando el pasillo de accesos. Las cámaras deberán realizar grabación con la detección de movimiento.

    El mantenimiento de las cámaras de video durante la ejecución del contrato estará a cargo EL CONTRATISTA.

Centros de Monitoreo y Gestión

17. Contar con un Centro de Monitoreo y Gestión encargado del monitoreo y atención de primer nivel de cualquier tipo de incidente que se presente en las plataformas de servicios.

18. Monitorear los servicios en tiempo real por medio de herramientas automatizadas que envían alarmas, generan y asignan casos en la herramienta de Mesa de servicio de acuerdo a su nivel de criticidad y cuya información permite generar acciones proactivas.

19. Monitorear 7X24 los recursos de los servidores de las aplicaciones, bases de datos y servicios, identificar disponibilidad e indisponibilidad, tiempos de respuesta y desempeño de cada aplicación. Emitir recomendaciones mensualmente para la optimización, realizar diagnósticos y análisis de seguimiento.

20. Generar alertas automáticas dirigidas al personal del ICBF bajo determinados eventos. El personal al que se le deben enviar las alertas y el tipo de eventos que las generan serán determinados por el ICBF en la Etapa de Transición y podrán ser modificadas en cualquier etapa del proyecto.

21. Configurar las acciones automáticas ante caídas del servicio, mediante envío de popup, e-mail, SMS, mensajes de consola, etc. El personal designado por el ICBF deberá recibir mensajes de notificación a los teléfonos móviles, cuando se presenten caídas de los Servicios, EL CONTRATISTA deberá asumir el costo de dichos mensajes.

22. Monitorear el uso de recursos lógicos de los dispositivos a través de los agentes activos instalados para tal efecto.

23. Identificar en forma temprana posibles fallas en los sistemas y dispositivos del servicio.

24. Actuar de inmediato ante la aparición de incidentes o alarmas para buscar su solución. El NOC (Network Operations Center) constituye un primer nivel de atención y deberá generar un caso para atención de segundo nivel.

25. Brindar Información al contratista de Mesa de Servicio y al ICBF en el caso de indisponibilidad de alguno de los servicios, de acuerdo al procedimiento establecido para tal fin.

26. Ejecutar y registrar la gestión realizada en la herramienta de Mesa de Servicios, frente a incidentes, problemas y cambios en el procesamiento, y cumplir con el escalamiento según corresponda y según lo especificado en el Manual de Procedimientos.

27. Aplicar los parches de mantenimiento de software preventivo y correctivo (parches, fixes o service packs) del software de monitoreo para corregir defectos.

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

28. Definir y mantener actualizada, en asocio con ICBF, la lista de contactos para el escalamiento del servicio de monitoreo.

29. Informar al contratista de mesa de servicio que administra la CMDB el ingreso de un nuevo hardware y software que soportan los sistemas de información del ICBF.

Seguridad Informática

Servicios de administración y operación:

30. EL CONTRATISTA debe garantizar la seguridad de la información del ICBF en todas sus sedes, a través de la implementación de soluciones a nivel tecnológico, alineados a los estándares y mejores prácticas de seguridad, aceptados internacionalmente y recomendados por los fabricantes de las tecnologías que serán implementadas para el cumplimiento de este contrato.

31. EL CONTRATISTA deberá suministrar, instalar, configurar, administrar, monitorear y dar soporte a los dispositivos de red necesarios para la protección perimetral del ICBF. También deberá administrar, apoyar la instalación, configuración y brindar soporte a las soluciones de seguridad, tanto existentes como nuevas que adquiera el ICBF durante el término del presente contrato.

32. EL CONTRATISTA deberá realizar actividades periódicas, las cuales deben incluir el estudio de tráfico en las redes tanto LAN como WAN con sus respectivos análisis de protocolos, deberá presentar un informe con los hallazgos de vulnerabilidades de seguridad obtenidos en dichos estudios, generar planes de acción y llevar a cabo las actividades necesarias para corregir dichos hallazgos. EL CONTRATISTA deberá realizar periódicamente tests de penetración (PenTest) para servidores, perímetro de red, bases de datos y aplicaciones, el alcance del pen test deberá acordarse con el ICBF previa su ejecución.

33. EL CONTRATISTA deberá diseñar un plan de trabajo para la instalación de actualizaciones y parches en servidores de aplicaciones y bases de datos productivas, en donde se minimicen los riesgos y se garantice la disponibilidad.

34. EL CONTRATISTA deberá brindar apoyo y proponer activamente recomendaciones al ICBF tendientes a incrementar el nivel de seguridad informática y al mejoramiento de la

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

protección de los servicios informáticos asociados a la infraestructura. Este apoyo derivará en planes de acción donde se detallen los requerimientos y actividades necesarias para aplicar dichas recomendaciones.

35. EL CONTRATISTA deberá dar un uso ético y protección a los accesos, contraseñas, información y recursos informáticos proporcionados por el ICBF, guardando estricta confidencialidad de la información sensible que pudiera llegar a manejar durante el desarrollo del presente contrato.

36. EL CONTRATISTA deberá alinear sus procesos al Sistema de Gestión de la Seguridad de la Información SGSI establecido en el ICBF y acatar todas las acciones y recomendaciones que de él se deriven.
37. EL CONTRATISTA deberá suministrar, instalar, configurar, afinar, monitorear y dar soporte a toda la tecnología necesaria para cubrir los requerimientos técnicos de seguridad descritos en este documento.

38. EL CONTRATISTA deberá cumplir con las normas y políticas de seguridad del ICBF.

39. EL CONTRATISTA deberá notificar al ICBF, a través del líder de Seguridad, cualquier incidente ocurrido sobre la infraestructura tecnológica.

40. EL CONTRATISTA deberá realizar acciones de respuesta a incidentes de seguridad, en coordinación con el ICBF a través del Líder de Seguridad Informática. Para ello, deberá generar un procedimiento de atención a incidentes, un plan de respuesta que conlleve a su solución, asumirá la investigación forense en caso de resultar necesario y presentará un informe de resolución de cada incidente. Esta información deberá alimentar una base de datos de conocimiento para la atención de futuros incidentes.

41. EL CONTRATISTA deberá retener y almacenar los logs relacionados con seguridad, por un periodo mínimo de 1 año.

42. EL CONTRATISTA deberá presentar un informe mensual de seguridad con el estado, avances, estadísticas y gestión de todos los temas de seguridad. Debe incluir evidencias del cumplimiento de los ANS y toda la información relacionada con la gestión de la seguridad informática del ICBF, el cual será definido y aprobado en conjunto con el ICBF.

43. Exchange Online tiene el servicio de EOP (Exchange Online Protection) que en conjunto con las reglas de flujo de correo garantizan la protección y filtrado de correo de toda la

organización, solución que debe ser administrada por EL CONTRATISTA y basada en las directrices de seguridad que estipule el ICBF. De la misma forma, EL CONTRATISTA deberá administrar la solución de antispam provista para el servidor Exchange On-Premise del ICBF.

44. EL CONTRATISTA debe definir, administrar y monitorear las políticas de actualización de parches para servidores, computadoras de usuarios finales y otros dispositivos actualizables como tabletas y móviles según sea el caso, por medio de WSUS o cualquier otra herramienta disponible para mantener actualizada la seguridad de los sistemas operativos.
45. EL CONTRATISTA deberá asesorar al ICBF en la implementación de requerimientos mínimos de seguridad y calidad en el manejo de la información a través de los medios y canales de distribución de servicios para sus beneficiarios y usuarios.

46. EL CONTRATISTA brindará soporte de segundo y tercer nivel sobre las soluciones de seguridad informática, la cual hace referencia a todas las soluciones e implementaciones de seguridad que estén instaladas y/o configuradas para asegurar la integridad, confidencialidad y disponibilidad de la información del ICBF.

47. EL CONTRATISTA deberá identificar, diagnosticar, solucionar y reportar problemas e incidentes de seguridad en la plataforma computacional a cargo. Para el cumplimiento de dicho fin EL CONTRATISTA debe elaborar un Plan de Respuesta a Incidentes, el cual debe contar como mínimo con la descripción de respuesta a un incidente, propósito del documento, alcance de los incidentes a los cuales aplica, definición de roles y responsabilidades para obtención de respuestas, procedimientos detallados de las medidas a tomar durante el incidente, diagnóstico, notificación del análisis, procesos de restauración (priorización de sistemas a recuperar) y evaluación de daños causados por el incidente.

48. EL CONTRATISTA deberá planear y desarrollar actividades periódicas mensuales en conjunto con el contratista de mesa de servicios que garanticen la máxima cobertura de actualizaciones de sistemas operativos y definiciones de antivirus en todas las sedes del ICBF, y presentará un informe mensual donde se muestren los porcentajes de cobertura en cada sede basándose en equipos totales contra equipos registrados en las consolas de administración de WSUS y antivirus, también deberá discriminar el porcentaje de equipos registrados que estén al día en cuanto a las actualizaciones. También, como parte de estas actividades, deberá mantener actualizados los firmwares de los dispositivos firewall.

49. EL CONTRATISTA debe definir parámetros de seguridad en servidores WEB, aplicaciones y servicios en internet para prevenir ataques a la disponibilidad, confidencialidad e integridad de la información de ICBF.

50. EL CONTRATISTA mantendrá a disposición de la Dirección de Información y Tecnología del ICBF, un directorio actualizado del personal de soporte especializado disponible, en el evento de ocurrencia de fraudes informáticos en los servicios que forman parte del alcance, será responsabilidad de EL CONTRATISTA, realizar el análisis forense, para lo cual deberá designar las herramientas y el personal certificado y calificado.
51. EL CONTRATISTA deberá adquirir y renovar 1 certificado digital wildcard que sirva para todos los servidores Web, las páginas públicas y otras aplicaciones del ICBF. El certificado debe ser tipo SSL (Secure Site - Secure Sockets Layer). También debe suministrar al menos un (1) Certificado tipo SSL SAN Geo Trust para correo Exchange 2010 o el equivalente para la versión de Exchange que en el momento se encuentre instalada. Los certificados deben ser emitidos por una Entidad certificadora válida y autorizada en Colombia. La línea Base de Certificados Digitales está disponible en el Anexo 001 – TABLAS LINEAS BASE. En caso de que el certificado wildcard no pueda ser instalado para el funcionamiento de alguna aplicación del ICBF, EL CONTRATISTA deberá suministrar el certificado digital apropiado.

52. EL CONTRATISTA debe implementar y documentar el procedimiento para el manejo, actividades y protocolos para la custodia y entrega de las contraseñas de administración. Estos procedimientos de custodia aplican para todos aquellos casos donde EL CONTRATISTA haga uso de cuentas y contraseñas de administración de las herramientas usadas para el cumplimiento de los servicios incluidos en el alcance de este proceso de selección, ejemplo, el firewall, consolas de antivirus, Bases de datos, aplicativos, IPS/IDS, Correo, Proxy, PC's y Servidores.

53. EL CONTRATISTA realizará las actividades preventivas y dispondrá de las herramientas orientadas a detectar, diagnosticar, evitar, reparar e informar sobre posibles fallas e incidentes de seguridad informática con el objetivo de prevenir incidentes que disminuyan la disponibilidad y desempeño requerido en la infraestructura de software, hardware, conectividad, comunicaciones y seguridad informática del ICBF. Estas actividades deben contemplar entre otras las siguientes:
    - Prevenir, detectar y corregir caídas en el software base, relacionadas a incidentes de seguridad tales como: sistemas operativos, motor de base de datos y aplicaciones.

- Prevenir, detectar y corregir caídas en los componentes de hardware, relacionadas a incidentes de seguridad tales como: servidores de datos, servidores de aplicación, racks, poniendo en ejecución el plan de contingencia. (Elaborado por EL CONTRATISTA).
- Prevenir, detectar y corregir caídas en los componentes de la red tales como concentradores y Routers teniendo en cuenta la implementación del plan de contingencia y DRP.
- Acordar con el ICBF las prioridades de solución concentrándose en los componentes críticos de la arquitectura de conectividad, comunicaciones, software, hardware y dispositivos de seguridad informática, esta priorización de componentes críticos, debe incluirse en el plan de Respuesta a Incidentes y en el Plan de Contingencia solicitado en este documento.
- Monitorear el desempeño de la red de comunicaciones, específicamente, monitorear el estado físico de la red y sus parámetros lógicos (tiempos de respuesta, balanceo de tráfico), verificando la existencia de los controles de seguridad requeridos para cada caso.
- Identificar, diagnosticar, solucionar y reportar problemas e incidentes para las soluciones proxy y antispam.

54. EL CONTRATISTA deberá diseñar el análisis de riesgos asociado a la infraestructura que disponga para la adecuada prestación de los servicios.

55. Actualmente el ICBF cuenta con el antivirus System Center Endpoint Protection 2012 administrado desde una consola centralizada. Será deber de EL CONTRATISTA administrar y soportar la solución de antivirus actual, planear y ejecutar labores que mantengan al mínimo el número de computadoras no gestionadas por la solución, o gestionadas pero no actualizadas con las últimas definiciones. En caso en que el ICBF decida cambiar dicha solución de antivirus, EL CONTRATISTA deberá la administración, configuración y soporte de la nueva solución, además de realizar las labores necesarias para la transición hacia ella.

Seguridad Perimetral (Firewall de Nueva Generación, IPS/IDS, VPN, filtrado de Navegación):

56. EL CONTRATISTA está en la libertad de diseñar la solución de firewall siempre y cuando cumpla con los requerimientos del ICBF descritos en este documento. Dicha solución debe abarcar un firewall para el Data Center Externo y otro para el Centro de Cómputo de la Sede de la Dirección Nacional del ICBF, manteniendo el requerimiento de configuración en alta disponibilidad solicitado. El diseño e instalación de los firewalls debe realizarse con el visto bueno del ICBF.

57. EL CONTRATISTA deberá diseñar, documentar y aplicar sobre la solución de firewall las políticas y reglas de seguridad asociadas a la infraestructura tecnológica. Además realizará la revisión, mantenimiento y actualización de políticas de común acuerdo y con la autorización del líder del servicio de seguridad informática del ICBF.

58. EL CONTRATISTA deberá realizar la administración, mantenimiento y actualización de los equipos de hardware que conformen la solución de firewall.
59. EL CONTRATISTA deberá otorgar, administrar, gestionar y brindar soporte a los accesos a través de conexiones VPN tanto user to site como site to site. El ICBF podrá solicitar dichos accesos sin que la cantidad de ellos le genere costos adicionales.

60. EL CONTRATISTA debe configurar, Implementar y administrar los controles de acceso lógicos que sean necesarios para proteger las redes y la información, en los servicios que apliquen y se encuentren relacionados en el alcance de este contrato.

61. Los controles de acceso lógicos deben estar asociados a Directorio Activo de Microsoft y deben cumplir con la política de filtros de navegación y filtros a nivel de firewall. Los accesos lógicos deben tener relacionada una cuenta de usuario de directorio activo con los privilegios establecidos de acuerdo al perfil al que pertenezca el usuario, esto se refiere a que no deben existir accesos a recursos informáticos sin la validación de privilegios.

62. EL CONTRATISTA debe mantener la Integración entre las soluciones proxy y la solución de administración de contenido de igual manera deberá Integrar las soluciones Proxy y control de contenido con la(s) solución(es) antivirus, antispyware y demás soluciones de seguridad que permitan mantener la disponibilidad, integridad y confidencialidad de la información de consulta de los usuarios.

63. EL CONTRATISTA debe integrar las soluciones proxy y control de contenido con los sistemas de autenticación del ICBF como el directorio activo.

64. EL CONTRATISTA debe realizar actividades de afinamiento de la solución proxy para permitir entre otras la optimización del cache de páginas visitadas por los usuarios para mantener el desempeño del servicio de sitios almacenados.

65. EL CONTRATISTA debe realizar la administración, mantenimiento, centralización y actualización de las políticas del filtro de navegación.

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

Obligaciones sobre la DMZ:

66. EL CONTRATISTA deberá crear, parametrizar, personalizar y dar acceso a los reportes que el ICBF considere necesarios en cualquiera de los dispositivos y herramientas de seguridad solicitadas en este documento.

67. EL CONTRATISTA debe realizar planes para la migración de servidores y aplicaciones a la DMZ, de común acuerdo y bajo aprobación del ICBF.
68. EL CONTRATISTA debe apoyar y realizar las labores técnicas necesarias para migrar servidores y aplicaciones a la DMZ.

69. EL CONTRATISTA deberá alinearse a las políticas de cambios y SGSI implementadas en el ICBF para realizar cualquier configuración o modificación sobre la DMZ.

70. EL CONTRATISTA debe realizar labores de configuración y soporte para mantener la DMZ en operación.

71. EL CONTRATISTA deberá notificar al ICBF, a través del líder de Seguridad, cualquier incidente ocurrido sobre la DMZ y los servidores y aplicaciones que se encuentren en ella.

Obligaciones sobre Pruebas de Penetración:

72. EL CONTRATISTA debe elaborar un plan de evaluación y de pruebas de penetración, el plan debe incluir por lo menos las fases de: Planificación, Ejecución y Post Ejecución. Dicho plan debe tener una política que enmarque las necesidades y cumpla con los objetivos de realizar las pruebas, poseer objetivos claros y alcanzables.

73. EL CONTRATISTA debe realizar las pruebas de penetración como mínimo dos veces al año, por lo menos en cuatro (4) segmentos de red. El ICBF puede solicitar que esta periodicidad y segmentos de red sean modificados según el resultado de las pruebas.

74. Las pruebas de penetración se realizaran sobre los servidores y aplicaciones del ICBF, y sobre plataformas suministradas por EL CONTRATISTA, que sean acordados con el ICBF durante la fase de planificación.

75. Fase de Planificación: La fase de Planificación del plan de evaluación debe recopilar la información de los activos que se encuentran en amenaza. ICBF entregará al CONTRATISTA el inventario de activos y su categorización, partiendo de esta

información EL CONTRATISTA debe priorizar los activos a los cuales se les realizaran las pruebas de penetración. En esta fase se tienen que identificar los activos que presentan vulnerabilidades. La fase de planificación debe elegir una técnica de aplicación de pruebas de penetración que cumpla con la política y objetivos de seguridad del ICBF y articularla con los objetivos de las pruebas de penetración incluyendo la verificación del sistema de seguridad. Debe incluirse los recursos que se necesitan para el desarrollo de las pruebas y el impacto que puede este puede tener al realizarse dichas pruebas sobre ambientes de producción. Se debe también tener identificados los sitios internos y/o externos, los responsables y tiempos para realizar evaluaciones y pruebas.

76. Fase de Ejecución: Durante la ejecución de la evaluación de la seguridad, las vulnerabilidades son identificadas por los métodos y técnicas definidas en la fase de planificación e identificadas en el plan de evaluación, esta etapa debe ejecutarse según la Etapa de Planificación.

77. En la Etapa de Ejecución debe obtenerse hallazgos, resultados e información que permita clasificar las vulnerabilidades, determinar la causa e identificar falsos positivos.

78. La ejecución de pruebas debe documentarse, por lo cual se deben ofrecer métodos de recolección y transmisión de información.

79. Fase de Post-Ejecución: La etapa de post ejecución EL CONTRATISTA debe entregar un informe con análisis y resultados en términos de vulnerabilidades, resultados de las pruebas de penetración, recomendaciones y acciones que mejoren la seguridad. El informe debe permitir tomar acciones correctivas, determinar la periodicidad de la ejecución del plan de evaluación y pruebas de penetración, debe permitir evaluar si la técnica elegida en la planificación es la correcta o deben generarse técnicas diferentes.

80. EL CONTRATISTA deberá tomar las medidas correctivas necesarias. El ICBF realizará validación de dichos correctivos antes y después de su aplicación con el fin de verificar que estos cumplen con lo requerido, con el fin de eliminar las fallas de seguridad detectadas y documentar los controles y soluciones implementadas. En caso de ser necesaria la adquisición de hardware para estos efectos, EL CONTRATISTA deberá presentar la propuesta técnica y económica al ICBF para su aprobación.

<u>Servidores</u>

Administración:

81. EL CONTRATISTA deberá administrar parámetros de los sistemas operativos de acuerdo con las mejores prácticas del fabricante y lineamientos dados por el ICBF.

82. EL CONTRATISTA deberá realizar el control de licencias de sistemas operativos para servidores de propiedad del ICBF, Mediante el uso de las herramientas que posee el ICBF – (KMS y System Center).

83. EL CONTRATISTA deberá generar un plan con el fin de que los logs de seguridad de los servidores queden en un repositorio centralizado el cual pueda ser indexado por una herramienta para la búsqueda de soluciones a incidentes presentados o consultados por el especialista de EL CONTRATISTA.

84. EL CONTRATISTA deberá verificar las bitácoras de errores, problemas y logs para búsqueda de causas de incidentes ocurridos y/o para prevenir su ocurrencia.

85. EL CONTRATISTA deberá instalar y configurar adecuadamente el software de Sistema Operativo y de aplicaciones de acuerdo a los requerimientos del ICBF y las mejores prácticas del fabricante.

86. EL CONTRATISTA deberá instalar, configurar, administrar y monitorear nuevo hardware y software para servidores que entre en operación durante el contrato, cuando el ICBF así lo requiera.

87. EL CONTRATISTA deberá realizar la instalación, configuración, administración y monitoreo a nivel de servidores, de servicios de escritorio (servicios de Impresión y scanning, políticas y demás publicados en Directorio Activo).

88. EL CONTRATISTA deberá mantener actualizados los servidores y sus sistemas operativos con los últimos niveles de firmware, parches y fixes ajustándose a cronogramas previamente aprobados con el ICBF.

89. EL CONTRATISTA deberá generar un plan para realizar la aplicación de nuevos parches de sistemas operativos en servidores de producción el cual debe someterse a una fase de prueba en máquinas dedicadas para ello, las cuales son suministradas por el ICBF.

90. EL CONTRATISTA deberá realizar la marcación de los servidores físicos de acuerdo a los lineamientos dados por el ICBF.

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

91. EL CONTRATISTA deberá administrar y monitorear el almacenamiento físico y lógico (Interno y externo) asignado al sistema operativo y a datos. Comprende actividades de planeación y ejecución de administración del almacenamiento de los servidores.

92. EL CONTRATISTA deberá administrar, monitorear y mantener durante la ejecución del contrato los espacios en disco, realizando depuración y/o generando la notificación al ICBF a que haya lugar para prevenir incidentes.

93. EL CONTRATISTA deberá generar informe bimestral con la lista de servidores sin utilizar en un período igual o mayor a 3 meses.

94. Configurar en todos los servidores objetos de monitoreo, los agentes necesarios para la apertura electrónica de tickets en la herramienta de gestión que se encuentre en operación en el ICBF.

95. El servicio debe incluir escalamiento de mantenimiento correctivo de equipos en garantía y diagnóstico de condiciones e infraestructura.

96. Si fueran necesarios equipos de contingencia en cuanto a Servidores, que hacen parte de la infraestructura soportada por EL CONTRATISTA, éste deberá suministrarlos a la entidad durante el tiempo requerido de acuerdo al incidente presentado.

97. Notificar al ICBF (líder designado del servicio) cualquier incidente que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible según la hora de aparición del incidente, y actuar proactivamente en la búsqueda y aplicación de la solución.

98. Garantizar el Servicio de manos remotas Encendido/Apagado de servidores localizados en el data center externo, previamente informado por el ICBF y otras actividades que lo requieran.

99. Diseñar, crear, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de Servidores.

100. Analizar, diseñar, proponer y ejecutar las configuraciones y arreglos de servidores necesarios para dotar de alta disponibilidad la plataforma de clusterización de servidores.

101. Instalar, configurar, administrar, monitorear y/o brindar apoyo al proveedor sobre el nuevo hardware de servidores y software que entre en operación durante el contrato, cuando el ICBF así lo requiera.

102. Analizar, diseñar, proponer y ejecutar las configuraciones necesarias previa verificación del ICBF de nuevos sistemas que optimicen procedimientos.

103. Analizar, diseñar, proponer y ejecutar el renombramiento de servidores previa autorización del ICBF.

104. Analizar, diseñar, proponer y ejecutar la redistribución de clusters, previa autorización del ICBF.

105. Generar los mapas lógicos de interconexión de servidores de aplicaciones y base de datos y mantenerlos actualizados.

106. Dar respuesta a las consultas técnicas realizadas por el ICBF, asesorando en el mejoramiento, estructura y ampliación de los servidores, con el fin de incluir nuevos servicios tanto para el cliente externo (servicios en Internet) como para el cliente interno, y respondiendo a las necesidades de crecimiento del ICBF en servicios y aplicaciones.

107. Documentar cada ticket (llamada de servicio, incidente o problema) relacionado con fallos de sistemas operativos y presentación del informe respectivo, así como dar apoyo en el diagnóstico de las causas de los mismos, independientemente del ambiente del servidor (Piloto, Desarrollo, Pruebas, Producción).

108. Proponer, coordinar y realizar cambios de sistema operativo, una vez analizados y aprobados por el Líder de Servidores y el Comité de Cambios del ICBF.

109. Mantener actualizadas las hojas de vidas de los servidores en un formato diseñado para ello en conjunto y presentarlas al ICBF cuando este lo requiera.

110. Mantener actualizado el listado de servidores, sus componentes y software instalado y suministrar la información al contratista de mesa de servicio con el fin de mantener la CMDB actualizada.

111. Llevar a cabo el análisis, diagnóstico y corrección de fallos y problemas técnicos presentados en hardware y en sistemas operativos y/o hacer seguimiento al proveedor o fabricante en el evento de que alguna solución requiera de tal escalamiento y presentar los informes correspondientes en un tiempo no superior a las 24H siguientes al incidente.

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

112. La plataforma de servidores debe estar disponible, administrada, monitoreada y en operación 7x24 y en concordancia con el Anexo 002 –TABLA LINEAS BASE.

113. Realizar pruebas tanto para la instalación, como para actualización y configuración de software de sistema operativo, siguiendo los lineamientos establecidos por el ICBF y mejores prácticas del fabricante.

Controladores de Dominio (DC)

114. EL CONTRATISTA deberá administrar las herramientas para el manejo de bases de datos de Directorio Activo, DNS, DHCP.

115. EL CONTRATISTA deberá administrar, monitorear, realizar actualizaciones y garantizar la adecuada replicación del Directorio Activo, DHCP y DNS.

116. EL CONTRATISTA deberá realizar las recomendaciones necesarias para que el sistema de Directorio Activo, DHCP y DNS funcione de la manera más adecuada.

117. EL CONTRATISTA deberá configurar y monitorear a nivel de sistema operativo y directorio activo las políticas de acceso a recursos, en seguimiento a las directivas emitidas por el ICBF (con fases de prueba y aplicación).

118. Administrar la seguridad de las plataformas en lo relacionado con los sistemas de autenticación (crear, deshabilitar, eliminar, modificar datos y cambiar claves a los usuarios).

119. Controlar y monitorear la frecuencia en fallos de autenticación de red (bloqueo) mediante el uso de una herramienta que permita el autocambiado de claves por olvido de la misma.

120. Controlar y monitorear la frecuencia de expiración y bloqueos por inactividad de cuentas de usuarios.

121. Analizar, diseñar, proponer y ejecutar las configuraciones y arreglos de servidores necesarios para dotar de alta disponibilidad la plataforma central de servicios básicos de red (Directorio Activo, DNS, DHCP).

122. Analizar, diseñar, proponer y ejecutar las configuraciones necesarias para el óptimo funcionamiento del Directorio Activo, DNS y DHCP, previa verificación del ICBF.

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

123. Hacer recomendaciones sobre mejores prácticas para la definición e implementación de políticas de seguridad, administración de usuarios, políticas de backup, políticas particulares de administración y otras que apliquen para la correcta administración de los servidores, sistemas operativos, el Directorio Activo, DHCP y DNS.

124. Garantizar la disponibilidad 7x24 de los recursos de la red (DNS, DHCP) y el acceso de los funcionarios (Directorio Activo), de acuerdo con los privilegios asignados por el ICBF.

Almacenamiento

Servicios de Administración y operación

125. Administrar el Almacenamiento SAN (Clariion CX4-240) y NAS (Celerra NX4) con el que cuenta el ICBF y el nuevo software y hardware de Almacenamiento que adquiera el ICBF durante el desarrollo del contrato.

126. Monitorear 7X24 las soluciones de Almacenamiento SAN (Clariion CX4-240) y NAS (Celerra NX4) con el que cuenta el ICBF, generando de manera automática en la herramienta de gestión de servicio, el registro de incidencias presentadas.

127. Administrar las herramientas (Analyser EMC, Thin Provisioning EMC, SAN Copy EMC, SnapView EMC, Fast Suite EMC,…etc.) con las que cuenta el Almacenamiento del ICBF para mejorar el acceso a los datos, aumentar el desempeño, reducir costos y garantizar la seguridad de los datos (creación y recuperación de copias de imágenes completas de los datos de producción en caliente.

128. El administrador de las soluciones de Almacenamiento SAN y NAS debe contar como mínimo con las siguientes certificaciones: Information Storage and Management (E10-001), VNX o Clariion Solutions Specialist Level (E20-390) y VNX o Clariion Solutions Expert Level (E20-885).

129. Apoyar a la Subdirección de Recursos Tecnológicos en la generación de conocimiento relacionada con el servicio, para su uso y registro en la base de datos de conocimientos de TI del ICBF, así como en la generación de propuestas sobre nuevos ANS o acciones que repercutan en la mejora del 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

130. Presentar Bimensualmente los siguientes reportes de comportamiento de la data basados en la herramienta Unisphere, Navisphere y Analyser: Comportamiento de WorkLoad, Distribución de WorkLoad, Medición a nivel de LUN, Medición a nivel de METALUN, Medición a nivel de StorageProcesor.

131. Apoyar en la implementación de soluciones nuevas relacionadas con el servicio, adquiridas a través de este contrato u otros inclusive.

Renovación del servicio de soporte 7x24 de las soluciones de almacenamiento SAN y NAS del ICBF

132. Adquirir para el ICBF la renovación del contrato de soporte 7X24 con el fabricante (EMC) de las soluciones de Almacenamiento SAN y NAS que vence 22/03/2015 y que cubra la duración del contrato.

Respaldos (Backup)

Servicios de Administración y operación

133. Administrar las herramientas de Backup de EMC Networker y Avamar, con las que cuenta el ICBF, con sus correspondientes módulos registrados.

134. Cumplir a cabalidad con lo definido por el ICBF respecto a la gestión de copias de seguridad y a la gestión para la restauración de copias de seguridad vigentes, junto a sus eventuales cambios que puedan presentarse durante el desarrollo del contrato.

135. Realizar el monitoreo 7x24 de las soluciones de respaldo, generando de manera automática en la herramienta de gestión de servicio, el registro de incidencias presentadas, tales como fallos en la ejecución de una tarea de respaldo enviando el respectivo mensaje de alerta para su pronto relanzamiento.

136. Desarrollar las actividades relacionadas con respaldo (backup) y restauración (restore) dejando registradas las acciones realizadas, en la herramienta de gestión suministrada por el ICBF.

137. Realizar, en coordinación con el servicio de administración de aplicaciones, el levantamiento de aplicativos y bases de datos a nivel nacional, determinando con los diferentes responsables la pertinencia de la creación, modificación o eliminación de las políticas de respaldo asociadas a estas.

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

138. Implementar, actualizar y ejecutar las políticas de backup y recuperación para servidores en los diferentes ambientes (desarrollo, pruebas, capacitación, pilotos y producción) y mantener actualizada mensualmente esta información.

139. Garantizar la realización de copias de seguridad de todas las aplicaciones, bases de datos, correo electrónico, repositorios del ICBF y plataforma de virtualización, así como la verificación y certificación de la correcta realización de las mismas, con la herramienta de respaldo de EMC Networker licenciada por el ICBF, de acuerdo a las políticas de Backup vigentes en el ICBF.

140. Atender las solicitudes respectivas a las políticas de Backup de la entidad (inclusión, modificación, retiro), especificadas a través del procedimiento descrito para tal fin y de acuerdo a los tiempos allí descritos.

141. Mantener y garantizar la política de rotación de medios utilizada por la entidad. El ICBF cuenta con una política de rotación de medios GFS (ABUELO, PADRE, HIJO), donde el backup perpetuo se mantiene indefinidamente, el anual se rota cada 5 años, el backup mensual, se rota cada año y el backup diario se rota semanal.

142. Coordinar internamente con el ICBF y la empresa encargada de la custodia externa de los medios, los tiempos de respuesta para la restauración de copias de seguridad en casos de contingencia como: daños de equipos, desastres naturales, robos, ataques malintencionados, siniestros fortuitos o en los casos en que el ICBF lo requiera.

143. Recibir medios magnéticos (CDs provenientes de las regionales y cintas de las tareas de respaldo centralizado), y remitirlos a la empresa de custodia externa de medios.

144. Efectuar la marcación de medios magnéticos de acuerdo con la nomenclatura y/o estándar del ICBF.

145. Suministrar las cintas requeridas (estimadas en 300 anuales, durante la ejecución del contrato) para realizar tareas de backup, las cuales deberán ser proporcionadas desde el inicio del contrato de outsourcing. Las cintas sobrantes que no sean utilizadas dentro del término de duración del contrato deberán ser entregadas al Almacén de la Dirección General del ICBF.

146. Mantener actualizada en documentación previamente concertada con el ICBF la información correspondiente como mínimo a:

- Inventario de medios
- Políticas de backup
- Información respaldada
- Consumo de medios de respaldo

147. Realizar por lo menos 2 veces al año, tareas de mantenimiento preventivo sobre las soluciones de backup con las que cuenta el ICBF, en conjunto con el fabricante de las mismas, registrando las actividades realizadas en una bitácora de actividades, las cuales hagan parte del informe de gestión mensual sobre el servicio.

148. Realizar actividades de restauración de pruebas, tanto a nivel de base de datos como de aplicación de los backup realizados, basado en un cronograma presentado anualmente y aprobado por la Subdirección de Recursos Tecnológicos del ICBF.

149. Apropiar los conceptos de la norma ISO27001 relacionados al servicio de respaldos, así como las mejores prácticas en gestión y gobernabilidad de TI (ITIL y COBIT).

150. Asegurar en todo momento, mediante soluciones de contingencia la toma de copias de seguridad íntegras de la información de la cual se solicite backup en las programaciones que se hayan solicitado, evaluando en caso de ser necesario la provisión de infraestructura o recursos adicionales a los existentes.

Servicios de custodia de medios

151. Contratar y mantener vigente durante la duración del presente contrato para el ICBF el servicio de custodia de medios, con una empresa especializada, la cual cumpla como mínimo con las actuales condiciones del actual contrato que el ICBF tiene a través del actual operador de TI (UT INDRA INTERNEXA).

Los requerimientos mínimos que se debe cumplir con el servicio de custodia externa son:

a. La temperatura y humedad relativa del ambiente en el que se deben encontrar almacenados los medios para su custodia están en el siguiente rango: Temperatura: 4°C a 32°C, Humedad Relativa: 20% a 80%, ambiente controlado con aire acondicionado.
b. Las cintas o medios resguardados deben colocarse en estantes o armarios adecuados en una biblioteca de cintas.
c. Los medios resguardados deben contar con un único código de identificación de la empresa de custodia de medios, que permita su

identificación y ubicación en los inventarios que la empresa de custodia de medios tenga.

d. Contar con la opción de asignar códigos diferenciados para rangos de cintas específicos, los cuales puedan ser enviados y/o solicitados por personas diferentes a los solicitantes de cintas sin codificación diferenciada.

e. Recibir como mínimo 1 vez a la semana los medios a ser enviados en custodia.

152. El servicio de custodia de medios debe comprender tanto el almacenamiento del medio, como el transporte desde el sitio de custodia hasta las instalaciones donde el ICBF tenga su infraestructura de respaldos y/o donde se requiera el recojo/entrega de información (por ejemplo CD's en la Sede de la Dirección General).

153. Informar inmediatamente sobre extravío, hurto o deterioro de los medios dentro de las 24 horas de ocurrido el suceso. En estos casos EL CONTRATISTA deberá asumir los costos de reposición respectivos.

154. Contar con la opción de servicio de transporte de emergencia disponible 7x24x365 con un tiempo no superior a 4 horas continuas en caso que se requiera.

Renovación del servicio de soporte 7x24 de las soluciones de respaldo del ICBF

155. Renovar durante la vigencia del contrato el soporte 7X24 de las soluciones de respaldo actuales del ICBF y todos y cada uno de los elementos de Hardware y Software que los compongan. La solución de respaldo en disco EMC AVAMAR vence el 30 de abril de 2015.

Servicios de migración de Backups históricos

156. El ICBF se encuentra estudiando la viabilidad de realizar la migración de todos sus históricos de información respaldados en la herramienta EMC Networker y alojado en cintas magnéticas LTO4, a soluciones emergentes, tales como servicios en la nube o respaldo en disco. En caso que esto se lleve a ejecución, EL CONTRATISTA deberá realizar las tareas de migración, de acuerdo a un cronograma previamente entregado por este y aprobado por el ICBF. Los costos asociados a esta obligación serán facturados como un ítem adicional a los servicios anteriormente descritos.

<u>Aplicaciones</u>

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

157. Planear, documentar y coordinar el despliegue y puesta en producción de la infraestructura para los proyectos de software, de acuerdo al procedimiento interno del ICBF de Puesta en producción de proyectos de software.

158. Proponer, diseñar configurar y administrar los esquemas de alta disponibilidad y balance para soportan las aplicaciones existentes o nuevas del ICBF.

159. Configurar, administrar, gestionar y monitorear (7x24) las aplicaciones en los ambientes producción.

160. Realizar labores de despliegue de aplicaciones, proponer e implementar soluciones y mejores prácticas de manera eficiente, efectiva y eficaz, trabajando en equipo con la Dirección de Información y Tecnología (DIT).

161. Entregar mensualmente, o por solicitud del ICBF, informes sobre los incidentes o mejoras que se efectúen sobre las aplicaciones y las acciones tomadas sobre cada caso.

162. Cumplir con las tareas y tiempos establecidos y acordados en los planes de trabajo para los proyectos que se presenten durante la vigencia del contrato.

163. Definir, implementar y documentar los ambientes de producción requeridos en los proyectos de software del ICBF de acuerdo a los procedimientos definidos por la DIT del ICBF.

164. Generar, implementar y documentar estándares para la instalación y administración de aplicaciones a nivel nacional en el ICBF.

165. Entregar al menos trimestralmente, o cuando lo requiera el ICBF, un documento con recomendaciones sobre las aplicaciones para mejorar las condiciones de seguridad, disponibilidad y desempeño de la infraestructura que soporta las aplicaciones.

166. Realizar diagnósticos y análisis de seguimiento.

167. Hacer seguimiento y documentar controles de cambios, controles de accesos, y actualización a las aplicaciones.

168. Generación de mapas de servidores de aplicaciones y actualización mensual de los mismos.

169. Mantener actualizado el inventario de Aplicaciones de acuerdo al formato establecido entre ELCONTRATISTA y el ICBF (Líder del servicio).

170. Realizar análisis detallado de incidente, gestión de problemas y actividades tales como análisis de tendencias, análisis de causa raíz y establecimiento de error conocido.

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

171. Administración de parches, y la gestión de configuración de la infraestructura de aplicaciones.

172. Proporcionar acceso a los logs de producción desde un repositorio centralizado sin necesidad de acceder a los sistemas de producción.

173. Suministrar estadísticas de uso y peticiones por aplicación.

174. Realizar Informes de análisis web donde se muestre, concurrencia por usuario, número de usuarios que visitan la aplicación (horas, días y por mes), páginas más solicitadas, cantidad de tráfico, duración de las visitas, Origen de la conexión, páginas de entrada y salida, código de respuesta (HTML) y concurrencia de usuarios.

175. Garantizar que las aplicaciones que sean administradas, contengan la documentación actualizada y completa.

176. Suministrar información de la utilización real del sistema comparada con las previsiones del Plan de Capacidad.

177. Garantizar que los resultados finales de los informes, revisiones del servicio y diagnósticos, que le sean encomendados, cumplan las especificaciones de calidad y plazos que se hayan acordado previamente para cada caso.

178. Proponer, diseñar, administrar, monitorear y configurar esquemas de alta disponibilidad que se requieran para el montaje de Clúster, NLB, balance por hardware u otros de similares o mejores características que determine EL CONTRATISTA, utilizando el hardware y el software proporcionado por el ICBF.

179. Proponer plan de trabajo anualmente en donde se contemplen acciones de mejora, soporte del negocio, mantenimiento y cualquier otro que considere tanto EL CONTRATISTA como el ICBF.

180. Proporcionar asesoramiento en riesgos, identificando puntos críticos y definiendo e implementando acciones.

181. En caso de que una sentencia, código o una mala configuración de una aplicación sea la causante del mal desempeño de una aplicación en producción, EL CONTRATISTA tiene la obligación de identificarla, probar que esa es la causa del mal desempeño de la aplicación en cuestión, e informar por escrito al ICBF, realizando el diagnóstico del problema y las recomendaciones pertinentes para su solución.

182. Atender las solicitudes y requerimientos respectivos al servicio de aplicaciones de la entidad (cambios, comunicación, configuración, despliegue, monitoreo).

183. Apoyar al ICBF en el diseño, implementación, medición y administración de pruebas piloto relacionadas con el servicio, contratadas a través de este contrato u otros.

184. Diseñar, suministrar y socializar plan de mantenimiento anual para el servicio de administración de aplicaciones.

185. Mantener actualizado la arquitectura del servicio.

186. Es responsabilidad de EL CONTRATISTA recopilar y guardar la información soporte para el cálculo de los indicadores (información estadística), esta información puede ser solicitada por la ICBF en cualquier momento.

187. Probar y monitorear el rendimiento de aplicaciones WEB. IIS ASP.NET por medio de trazas, contadores de desempeño, rendimiento u otro método que permita hacer un seguimiento de la ejecución de las aplicaciones y del código de una página o aplicación, como resultado de estos se debe generar un informe en donde se muestren recomendaciones junto con un plan de acción donde se detallen los requerimientos y actividades necesarias para aplicar dichas recomendaciones.

188. Administración, operación, monitoreo y mantenimiento de la plataforma de aplicaciones, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en estado de operación óptima las aplicaciones del ICBF.

189. En caso que sea requerido diseñar, implementar y administrar soluciones de virtualización de aplicaciones tanto actuales como otras nuevas inclusive, a través del hardware y software suministrado por el ICBF.

Base de datos

190. Realizar y garantizar la correcta Migración de los motores de base de datos o componentes de estos a versiones más recientes asociados a atención de requerimientos, cambios e incidentes.

191. Desarrollar, documentar e implementar planes de mantenimiento. Las tareas de mantenimiento se podrán verificar a través de los archivos de log de ejecución y serán enviadas según solicitud del ICBF.

192. Instalar, administrar y soportar bases de datos Oracle, Application Server OAS, Oracle Estándar Edition 10g o superior y Forms and Reports Services 10g o superior, administrar y configurar RMAN.

193. Administrar, configurar y automatizar tareas de mantenimiento y optimización de los motores de bases de datos a través de la herramienta que EL CONTRATISTA suministre.

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

194. Creación y administración de trabajos automáticos en los motores de base de datos relacionados con tareas de mantenimientos y requerimientos efectuados por el ICBF, garantizando la correcta ejecución, dejando como evidencia los logs.

195. Realización de tuning a través de las herramientas del motor u otra en los diferentes ambientes que tiene dispuesto el ICBF y de acuerdo a los requerimientos realizados por el ICBF.

196. Analizar y documentar instrucciones Transact-SQL mediante el asistente para la optimización de motor de base de datos (MS SQL Server), utilizando trazas, tablas de traza o secuencias de comandos Transact-SQL. De acuerdo al resultado, realizar las recomendaciones e implementarlas de según al procedimiento de control de cambios.

197. Recomendar la mejor combinación de índices en las bases de datos mediante el uso del optimizador de consultas para analizar las consultas de carga de trabajo y en conjunto con el ICBF, verificar la viabilidad de su implementación.

198. Analizar planes de ejecución (MS SQL Server), sobre consultas, con el fin de identificar y corregir cuellos de botella.

199. Gestionar, configurar y administrar las herramientas de rendimiento de MS SQL Server.

200. Utilizar las herramientas de Microsoft SQL Server para supervisar los eventos de SQL Server y para optimizar el diseño de la base de datos física como son:
    - Analizador de SQL Server.
    - Monitor del sistema para supervisar el uso de recursos.
    - Monitor de actividad de SQL Server Management Studio.
    - Uso de los procedimientos almacenados de Transact-SQL que crean, filtran y definen trazas.
    - Supervisar los registros de errores.
    - Uso de los procedimientos almacenados del motor de base de datos (Transact-SQL), como son sp_who, sp_lock, sp_spaceused, sp_monitor, entre otros.
    - Instrucciones DBCC (Comandos de consola de base de datos) para comprobar estadísticas de rendimiento y coherencia lógica y física de una base de datos.
    - Funciones (Transact-SQL), para mostrar estadísticas de instantáneas acerca de la actividad de SQL Server desde el inicio del servidor.
    - Marcas de traza (Transact-SQL), para diagnosticar problemas o causas de bajo rendimiento (por ejemplo, cadenas de interbloqueos en el servidor).
    - Optimizar el diseño físico de las bases de datos, mediante el Asistente para la optimización de motor de base de datos.

201. Gestionar y administrar las herramientas de configuración como:

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

- Configuración de superficie de SQL Server.
- Informe de uso y errores de SQL Server.
- Símbolo del Sistema de Notification Services.
- Configuración de reporting services, integration services, analysis services y business Intelligence.

202. EL CONTRATISTA deberá llevar el control de las licencias del motor de base de datos SQL Server adquiridas versus las utilizadas por el ICBF.

203. Monitorear (7X24) los recursos de los servidores de base de datos, identificar cuellos de botella, emitir recomendaciones mensualmente para la optimización de consultas, realizar diagnósticos y análisis de seguimiento.

204. Monitorear las tareas programadas (7X24) creadas en los motores de base de datos e informar oportunamente las fallas presentadas emitiendo un diagnóstico y recomendación.

205. Deberá realizar un Informe mensual sobre el comportamiento de la base de datos que incluya como mínimo: informe de bloqueos (deadlock), recomendaciones, comportamiento estadístico de índices, recomendaciones para particionar tablas, vistas, top 100 de sentencias que consuman más recursos.

206. Llevar bitácora de control de las bases de datos y sus componentes del ICBF, incluyendo como mínimo crecimiento mensual, incidentes, ejecución de backup, tareas automáticas, análisis de errores, optimización de procesos y alertas.

207. Establecer, documentar e implementar en conjunto con el ICBF las políticas de acceso para cada una de las bases de datos.

208. EL CONTRATISTA es responsable de realizar los traslados físicos de las bases de datos, bajo solicitud y aprobación del ICBF durante la duración del contrato, mediante un proceso de control de cambios, previa aprobación del comité de control de cambios.

209. Estandarizar la ubicación física y lógica de las bases de datos en todos los equipos servidores y estaciones de trabajo del ICBF, generando instalaciones de acuerdo a las mejores prácticas recomendadas por los fabricantes de las bases de datos.

210. Documentar, mantener actualizada y entregar al final del contrato o cuando se requiera en formatos acordados con el ICBF, la base de datos del conocimiento y de configuraciones en cada servidor de base de datos: Gestión de configuración, Gestión de problemas, Gestión de cambios entre otras.

211. Generar alertas cuando el servicio no esté disponible o se presenten fallas, documentar los incidentes, acciones realizadas y planes de mitigación de riesgos.

212. Mantener actualizado el inventario de Base de Datos de acuerdo a los formatos establecidos en conjunto con el ICBF.

213. Gestionar el creciente tamaño de las bases de datos y diseñar los planes apropiados para administrarlos

214. Velar por que se cumplan los tres pilares de la seguridad de la información, la Confidencialidad, Integridad y Disponibilidad.

215. Manejo de desastres que incluye toda la planificación, organización y pruebas de los planes de contingencia y procedimientos de recuperación de base de datos.

216. Aplicación continua de las políticas, procedimientos y estándares para la creación, uso, distribución y eliminación de datos en las Base de datos. EL CONTRATISTA debe definir, documentar y comunicar las políticas, procedimientos y estándares antes de ser publicados.

217. Documentar las causas y acciones a tomar en aquellas bases de datos que estén por debajo del 100% en disponibilidad.

218. Realizar el Restore cuando se requiera de las bases de datos de los diferentes ambientes con las que cuenta actualmente el ICBF, así como aquellas bases de datos que se adquieran durante la vigencia del contrato.

219. Proponer, documentar, asesorar e implementar soluciones y mejores prácticas, entregar mensualmente, o antes si se requiere, informes sobre los incidentes que se presenten sobre las bases de datos, recomendaciones y acciones tomadas sobre cada caso.

220. Ejecutar una aplicación que permita trimestralmente identificar en los equipos personales de los Colaboradores del ICBF si tienen herramientas SQL server instaladas y entregar un informe detallado de los equipos que se detecten con dichas herramientas.

221. Generar cronograma de las actividades de mantenimiento con fechas de ejecución y responsables de la ejecución.

222. EL CONTRATISTA deberá brindar apoyo y proponer activamente recomendaciones al ICBF tendientes a optimizar el uso de recursos, asegurar la disponibilidad, seguridad, seguimiento, control, continuidad, operación y buen desempeño de las base de datos del ICBF. Este apoyo derivará en planes de acción donde se detallen los requerimientos y actividades necesarias para aplicar dichas recomendaciones.

223. EL CONTRATISTA debe designar personal especializado que se encuentre disponible de forma permanente (7x24) para responder a las alertas y/o incidentes generados en la plataforma tecnológica, y que afecte el servicio de base de datos.

224. Notificar al ICBF cualquier incidente que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible según la hora de aparición del incidente, y actuar proactivamente en la búsqueda y aplicación de la solución.

225. Diseñar, crear, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de base de datos.

226. Dar respuesta a las consultas técnicas realizadas por el ICBF, asesorando en el mejoramiento y optimización de recursos, con el fin de garantizar la disponibilidad y buen desempeño de las base de datos

227. Apoyar a la Subdirección de Recursos Tecnológicos en la generación de conocimiento relacionada con el servicio, para su uso y registro en la base de datos de conocimientos de TI del ICBF.

228. Desarrollar un plan de capacidad como mínimo una vez al año, donde se evalúe el planteamiento de la suficiencia de la infraestructura para las bases de datos, así como la pertinencia de realizar mejoras o acciones que repercutan en la mejora del servicio.

229. Administración, operación, monitoreo y mantenimiento de la plataforma de base de datos, así como la ejecución de todas las tareas recurrentes, programadas y no programadas para mantener en estado de operación óptima las base de datos del ICBF.

Telefonía IP

Administración del servicio de Telefonía IP

230. Garantizar la continuidad de la operación de los servicios de Telefonía IP de la entidad.

231. Administrar, gestionar configurar y monitorear los servidores, gateways y demás componentes que conforman la solución de telefonía IP del ICBF.

232. Realizar labores de administración a la solución de telefonía IP tales como: creación de usuarios, creación de extensiones, configuración de terminales IP, configuración de softphone, configuración de clientes UC700 Desktop, configuración de clientes MC550 Smartphone, configuración de fax IP, asignación de permisos, asignación de bolsas de minutos, generación de reportes de tarificación y demás componentes con los que cuente la solución.

233. Mantener actualizada y depurada la base de datos con la información de los usuarios de la planta telefónica y comunicaciones unificadas.

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

234. Brindar soporte técnico telefónico sobre la plataforma de telefonía IP a los Ingenieros de las Sede Regionales e Ingenieros de Soporte cuando estos lo requieran.

235. Identificar líneas análogas en el strip telefónico y centros de cableado de la sede de la Dirección General.

236. Realizar la conectividad y restablecimiento de líneas análogas, fax análogas en la sede de la Dirección General cuando se requiera.

237. Brindar soporte a los usuarios sobre el cliente UC700 Desktop y MC550 Smartphone.

238. Generar reportes estadísticos de acuerdo a las necesidades de la entidad (tarificación por usuario, por dependencia, por sede).

239. Velar por la seguridad de la información del sistema de telefonía IP generando copias de seguridad de la configuración de la planta y equipos relacionados, de la base de datos de usuarios y todos los demás relacionados con el servicio.

240. Mantener actualizada la información del inventario de la infraestructura tecnológica del servicio de Telefonía IP.

241. Documentar los tickets que sean creados a través de la mesa informática de soluciones (MIS) del ICBF, a través de los cuales se reporten incidentes, requerimientos o cambios.

Office 365

Las siguientes obligaciones son aplicables a todos los servicios contemplados para Office 365.

242. EL CONTRATISTA deberá Garantizar la administración, gestión, configuración, operación, monitoreo y control de la plataforma de Office 365.

243. Realizar la gestión con fabricante, realizar el mantenimiento, migración, upgrade de la infraestructura, sus servicios, componentes y/o unidades lógicas en caso de ser requerido.

244. EL CONTRATISTA deberá realizar Migración en caso de ser requerida de toda la infraestructura que forma parte de Office 365 en el ICBF y sus respectivas unidades

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

lógicas y operativas pertinentes en cada servicio, como Servidores, Sistemas Operativos, Plataformas, aplicativos, servicios, usuarios, grupos, sitios, reglas entre otras, propias de cada servicio y/o producto.

245. EL CONTRATISTA deberá hacer upgrade de versión en caso de ser requerido durante la ejecución del contrato, teniendo en cuenta los procedimientos establecidos por el comité de control de cambios, en los casos que ICBF lo solicite. El ICBF suministrara el debido software licenciado para este fin.

246. EL CONTRATISTA deberá garantizar la administración, operación, soporte, Mantenimiento y Migración (en caso de ser requerido) de cada uno de los servicios de Office 365 de acuerdo a las guías y procedimientos que se definan para este fin por el ICBF en acuerdo con EL CONTRATISTA.

247. Administrar el licenciamiento asignado para el funcionamiento de la Infraestructura y los servicios de Nube, las licencias solo se podrán asignar o retirar bajo la aprobación del ICBF.

248. Garantizar el acceso y sincronización de los servicios en los dispositivos de comunicación que requiera el ICBF de acuerdo a sus necesidades durante la ejecución del contrato.

249. Garantizar el acceso a la plataforma OWA (Outlook Web Access) a través de un navegador – servicio web.

250. Generar los mecanismos necesarios para el monitoreo de la infraestructura de Office 365.

251. Informar semanalmente al ICBF el estado de los servicios y/o disponibilidad de la plataforma, reportando comportamiento detallado de problemas y/o incidencias generadas durante el periodo, con las posibles acciones correctivas a implementar, también se debe incluir el análisis de los informes y graficas que la plataforma de Office 365 arroja.

252. En el caso de que EL CONTRATISTA suministre herramientas para el apoyo de la administración, soporte y gestión de los servicios, se requiere que el tipo de autenticación sea única “single sign-on”, mediante sincronización con el Directorio Activo de Microsoft.

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

253. Brindar acceso pertinente a los distintos módulos, y/o via Powershell al ICBF, para consultar o auditar los distintos servicios.

254. Gestionar y documentar los incidentes en la herramienta definida por el ICBF con la información pertinente, en los tiempos establecidos.

255. Contar con aplicaciones que permitan la administración de los servicios On-premise; y demás funcionalidades adicionales, para tener completa visibilidad sobre los servicios prestados al ICBF, así como de la trazabilidad de todas las actividades de administración, estas aplicaciones pueden ser de terceros, o del fabricante de la solución, y se debe dar acceso en caso de ser requerido al ICBF, este ítem no debe representar costos adicionales para la entidad.

256. Entregar los logs o evidencias requeridas por el ICBF, para cualquiera de los servicios de Office 365 contenidos en el presente documento de acuerdo a las políticas y/o disponibilidad de Logs de acuerdo a las especificaciones o conceptos emitidos por el fabricante.

257. Programar, ejecutar y documentar los resultados del proceso de Help Check, de todos los roles y parámetros que conforman la Infraestructura On-premise y Online de Office 365 una vez al año.

258. Configurar e implementar las políticas de backup incrementales y totales periódicos de: configuraciones, bases de datos, sitios, objetos, repositorios, logs de los servicios de Office 365 tanto On-premise como Online (si se disponen), sin que esto implique afectación alguna al servicio.

259. Ejecutar labores de mantenimiento periódicas sobre las bases de datos, Medios de Almacenamiento, estructuras lógicas y físicas de los servicios que dependan de las mismas a nivel On-premise.

260. Notificar al ICBF (líder del servicio) cualquier incidente que afecte la prestación de Office 365 y de los servicios conexos, a través de los medios disponibles según la hora de aparición del incidente y dejar registro de la notificación, para lo cual deberá brindar la solución de cualquier incidente de manera inmediata y efectiva sin más espera que la implementación que la solución demande.

261. Administrar, configurar y monitorear la plataforma BES (Blackberry Enterprise Server) Online para el acceso de dispositivos Blackberry a Office 365.

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

Servicios de Sincronización y Federación para Office 365

262. Administrar, configurar, gestionar y monitorear la infraestructura destinada para los servicios de sincronización y federación del servicio On-premise y Office 365.

Servicio de Correo (Exchange On-premise – Exchange Online)

263. Administración del servicio de correo e infraestructura de Exchange Server (On-premise) y Exchange Online a través de los medios y herramientas suministrados por el fabricante y/o que vengan disponibles en la plataforma. El uso de herramientas no avaladas por el fabricante debe ser autorizado por el ICBF.

264. Proveer los medios para la distribución masiva de mensajes de correo hacia cuentas externas (NO ICBF) ya sea por medio de herramientas y/o plataformas externas (de suscripción mensual o anual), o propias del proveedor. Estas herramientas no deben afectar la reputación del dominio del ICBF y deben garantizar el enmascaramiento del origen para garantizar la confianza del destinatario en caso de no ser remitidos los mensajes desde la plataforma del ICBF tanto On-premise, como nube.

265. Garantizar el acceso vía web a los buzones On-Premise mediante protocolo seguro, a través de navegadores como Microsoft Internet Explorer, Mozilla Firefox. Safari, Google Chrome, indicando las versiones soportadas, que están sobre la infraestructura On-Premise.

266. Gestionar las respectivas tareas técnicas que permitan garantizar el acceso a los servicios, utilizando el nombre MX que disponga el ICBF, que será la URL dispuesta por la Entidad para acceder vía web a los servicios de correo On-premise en caso de ser requerido.

267. Configurar filtros y redirección de mensajes a carpetas personales o archivados locales en caso de ser requeridos.

268. Garantiza la configuración y ajustes de usuarios de Exchange Online acorde con la configuración del servicio del DNS, y Autodiscover de correo.

269. Crear y gestionar las listas de distribución, que el ICBF requiera de acuerdo a sus necesidades.

270. Proporcionar la delegación en la administración de buzones (Superior – subalterno) o retirar los mismos. Los procedimientos deberán establecerse entre EL CONTRATISTA y el ICBF.

271. Controlar los parámetros de correo mediante políticas de Exchange, modificación de privilegios autorizados por el ICBF (tamaño buzones, número destinatarios máximo, delegaciones), administración de almacenamiento según la plataforma que corresponda.

272. Administrar, Gestionar, configurar, monitorear y soportar la herramienta EOP y las reglas de flujo de correo, las configuraciones de reglas de flujo de correo deben aplicarse de común acuerdo y bajo aprobación del ICBF.

273. Realizar los ajustes de configuración y requerimientos o incidentes que se generen sobre de la plataforma de correo en sus servicios de filtrado, flujo de correo y EOP (Exchange Online Protection) bajo los lineamientos destinados para tal fin y para garantizar el flujo apropiado de los mensajes entrantes y salientes del dominio ICBF.

274. Realizar los respectivos Backups de Buzones cuando los mismos expiren o se solicite explícitamente por el ICBF a través de la Mesa de Servicio o cuando apliquen los respectivos lineamientos para este tema.

Servicio de Mensajería Instantánea Lync (On-premise – Online)

275. Garantizar el funcionamiento y operación de la Infraestructura Lync On-premise y su federación con la nube y todos los servicios asociados o derivados como lo puede ser chat Pc-to-Pc y múltiples clientes, Videoconferencias, llamadas, presentaciones, compartir archivos, compartir escritorios, federación con otros dominios y garantizar la debida operación de los servicios Lync-online y Lync-On-premise.

276. Administrar la infraestructura On-premise, y los servicios Online que el ICBF tiene destinados para este servicio.

277. Garantizar el acceso a través de Internet al servicio de Lync fuera del dominio ICBF.

Servicio SharePoint (On-premise – Online)

278. Realizar la creación, modificación, administración de sitios y subsidios otorgando los permisos que requiera el ICBF, acordes al organigrama del instituto, o a los sitios/subsitios que se autoricen por parte del ICBF.

279. Administrar la Infraestructura On-premise y los servicios de nube pertenecientes al ICBF para la operación de este servicio.

280. Suministrar herramienta de gestión para Sharepoint Online, que permita administrar, realizar, restablecer, backups de sitios y aplicaciones de Sharepoint Online, y que permita la migración de sitios y aplicaciones entre la infraestructura On-premise y Online a partir de la versión Sharepoint Sever 2013 y SharePoint Online.

Servicio de Yammer

281. Administrar, configurar, gestionar y monitorear la infraestructura On-premise que el ICBF tenga destinada para la operación del servicio.

<u>Herramientas de Gestión y Monitoreo</u>

282. En la actualidad el ICBF cuenta con las siguientes herramientas de monitoreo y gestión.

- Unisphere, Navisphere, Analyser EMC, Thin Provisioning EMC, SAN Copy EMC, SnapView EMC, Fast Suite EMC. Las cuales se encuetran en producción.

- Microsoft System Center:

  - la solución está completamente licenciada para los siguientes módulos:

    - Configuration Manager + Endpoint Protection
    - Service Manager
    - Operation Manager
    - Virtual Machine Manager
    - Data Protection Manager
    - Orchestrator

  De las cuales se encuentran en operación actualmente, Configuration Manager + Enpoint Protection, Virtual Machine Manager.

  De los cuales se encuentran en operación actualmente, Configuration Manager + Enpoint Protection, Virtual Machine Manager, WSUS (Capitulo de Seguridad), KMS (Capitulo de Servidores) los cuales deben ser gestionados, administrados y monitoreados en todas sus

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

funcionalidades y módulos por EL CONTRATISTA con personal idóneo para este fin.

En caso que no están implementadas y en caso de requerirse explícitamente por el ICBF, EL CONTRATISTA debe implementarlas con personal certificado en las mismas, suministrando información o reportes que sobre ellas se soliciten. El ICBF proveerá toda la infraestructura física requerida única y exclusivamente para herramientas que son de su propiedad.

283. EL CONTRATISTA deberá implementar y operar el módulo System Center Operations Manager para el monitoreo y control de la infraestructura el ICBF.

284. EL CONTRATISTA deberá usar la Suite System Center para cumplir los requerimientos del presente documento a nivel de herramientas, en caso de necesitar algún módulo de System Center no implementado, EL CONTRATISTA podrá implementar y operar el mismo el pro del beneficio y utilización de herramientas propias del ICBF.

285. El ICBF podrá solicitar la implementación y/o modificación, Técnica, Funcional y operativa de cualquiera de los módulos de la Suite System Center,

286. Toda implementación, modificación y/o configuración, bases de datos que estén sobre System Center, será total propiedad del ICBF, las mismas deben alinearse a los procedimientos y lineamientos que el ICBF disponga para tal fin, debe cumplir con las buenas practicas del fabricante y al final del contrato deben ser entregadas debidamente documentadas.

287. EL CONTRATISTA podrá utilizar System Center para resolver cualquiera de los requerimientos del presente capitulo, siempre y cuando la herramienta lo realice de forma nativa o con los modulos certificados por fabricante para este fin (Configurations u Management Packs), en caso de que el modulo o la funcionalidad no este implementada EL CONTRATISTA deberá implementarla, administrarla y gestionarla, con el personal idóneo y aprobado por el ICBF; Antes y durante la implementación de cualquier modulo debe realizar las integraciones pertinentes con otros servicios y/o contratos dentro del marco del presente contrato, toda implementación y/o acción debe quedar debidamente documentada.

288. En caso de que la Suite System Center o las herramientas antes expuestas no cumplan algún requerimiento del presente capitulo, EL CONTRATISTA deberá suministrar las herramientas adicionales que considere necesario para el cumplimiento

del presente previo concepto-consulta técnica del fabricante de las herramientas que están como propiedad del ICBF donde se evidencie el no cumplimiento del requerimiento específico.

289. Para implementación de toda herramienta propietaria u ofrecida por EL CONTRATISTA en el marco de las obligaciones del presente contrato, EL CONTRATISTA deberá suministrar toda la infraestructura, Licenciamiento, Bases de Datos, Sistemas Operativos, recursos físicos o lógicos necesarios para el funcionamiento de las herramientas que sean de su propiedad, o que use en el marco de la ejecución de este contrato.

290. EL CONTRATISTA deberá integrar las herramientas del ICBF y las que suministre EL CONTRATISTA con la aplicación de Mesa de Servicio, de acuerdo a la herramienta que el proveedor de ese contrato suministre.

291. EL CONTRATISTA deberá suministrar al menos dos (2) Televisores de 50 pulgadas de tecnología LED, y conexión HDMI, Widi (accesorio), Conexión RG45 y WiFi, con los equipos requeridos para prestar el servicio de Dashboard que permita identificar el estado actual de los servicios del ICBF, este servicio podrá contar con la opción de consulta desde una dirección web, al final del contrato las pantallas y sus elementos deberán quedar para el ICBF.

292. EL CONTRATISTA deberá participar activamente con los demás proveedores (Redes y Mesa de Servicios) en la integración de todas las herramientas de gestión y monitoreo y las provistas por el ICBF. Esta integración debe permitir la gestión de eventos y alarmas en tiempo real para la creación automática de tickets y las notificaciones al personal designado por el ICBF.

293. En el momento en que el ICBF adquiera alguna herramienta o plataforma adicional, o que sea de su propiedad actual, ésta deberá ser implementada y/o integrada por EL CONTRATISTA a sus herramientas de gestión y monitoreo, siempre y cuando la herramienta adquirida por el ICBF lo permita y sea solicitado expresamente por el ICBF, la infraestructura requerida para esto será suministrada por el ICBF únicamente para plataformas o herramientas propias.

294. EL CONTRATISTA debe programar y realizar capacitaciones y transferencia de conocimiento con una duración mínima de 40 horas en lo que concierne a la operación, dirigidas al menos para 25 personas designadas por el ICBF, donde se incluya: herramientas de gestión, monitoreo y diagnóstico, nuevas tecnologías provistas por EL

CONTRATISTA y las demás herramientas que se utilicen durante el desarrollo del proyecto.

295. Las capacitaciones deben realizarse de manera periódica cuando existan actualizaciones sobre las herramientas o cambios en el personal designado por el ICBF.

296. EL CONTRATISTA deberá gestionar la administración y monitoreo de todos los Ítems solicitados en el capítulo 6.10 HERRAMIENTAS DE GESTION Y MONITOREO a través de las herramientas propias del ICBF o suministradas por el contratista en caso de ser necesario, permitiendo generar esquemas de monitoreo personalizables y accesibles.

297. EL CONTRATISTA debe Monitorear y Administrar el Licenciamiento del ICBF a través de las Herramientas que el ICBF disponga para este fin, como lo es el caso de KMS Server, y las que el ICBF adquiera para este fin durante el transcurso del Contrato.

Administración y Monitoreo de Puntos Finales

298. EL CONTRATISTA debe gestionar el monitoreo para todos los End Points del ICBF a través de las herramientas propias del ICBF o suministradas por el contratista en caso de ser necesario, permitiendo generar esquemas de monitoreo personalizables y accesibles.
299. EL CONTRATISTA deberá gestionar el adecuado descubrimiento automático de hardware y software de la red de ICBF, de tal manera que se almacene y actualice de manera automática el inventario en una base de datos centralizada (CMDB). La CMDB será suministrada y administrada por el contratista de mesa de servicio. Adicionalmente deberá contener detalles de cada ítem o elemento de configuración de la infraestructura tecnológica y debe permitir la relación entre ellas y las incidencias, problemas, cambios y otros datos del servicio de TI, garantizando así, contar con la información actualizada.
300. EL CONTRATISTA administrara a nivel lógico todos los end points que puedan estar conectados al Directorio Activo, o que sean suministrados por el mismo, y se regirán bajo los lineamientos que el servicio de directorio activo disponga para este fin.
301. Actualmente el ICBF cuenta con un servidor Microsoft KMS para administración del licenciamiento Microsoft, por lo tanto EL CONTRATISTA debe administrar, gestionar, monitorear y soportar el licenciamiento de todos los end points del ICBF usando el KMS y suministrar las demás herramientas necesarias para administrar el licenciamiento que no esté cubierto por el servidor KMS.

Monitoreo y Administración Centralizada a Través de SNMP de las UPS a Nivel Nacional.

302. El CONTRATISTA debe realizar el monitoreo y administración centralizada a las UPS de la Entidad, las cuales se encuentran ubicadas en diferentes sedes a nivel nacional, esto a través de protocolo SNMP. Actualmente el ICBF utiliza el software de monitoreo SPICEWORKS NETAGENT versión 2013, versión Free, pero EL CONTRATISTA puede suministrar un software de Iguales o Superiores condiciones, software que sea compatible con cualquier UPS, el software deberá ser administrado por EL CONTRATISTA.
303. El objeto de contratar el monitoreo y administración de las UPS, es anticiparse a las fallas que puedan presentar las UPS, a través del monitoreo permanente de los parámetros y la generación de warning, alertas y alarmas, las cuales deben ser detectadas en primera instancia por el CONTRATISTA, esto le permitirá realizar acciones correctivas y tomar decisiones.
304. El monitoreo y administración de las UPS será realizado por el CONTRATISTA en sus instalaciones e infraestructura tecnológica a través de un NOC.
305. El supervisor del contrato o quien este designe, deberá poder verificar a través del software Centralizado de monitoreo y administración el estado de las UPS en tiempo real (a través de una interfaz web y a través de alertas vía correo electrónico y mensajes de texto vía celular), permitiendo a la Entidad identificar en línea las fallas o inconvenientes que se presentan con las UPS. De esta forma, se podrán medir los tiempos de respuesta del contratista de UPS frente a la presencia de una falla o eventualidad. Teniendo en cuenta lo anterior, el CONTRATISTA deberá asignar un mínimo de 3 usuarios de consulta para realizar dicha verificación y seguimiento.
306. A través de los SNMP el CONTRATISTA y el líder de servicios de UPS del ICBF podrá monitorear ON LINE a través de una conexión a internet, a través de un usuario y contraseña la información actualizada presente en cada UPS relacionada con: voltajes de entrada y salida, voltaje de las baterías, capacidad de la UPS, temperatura, estatus AC, estatus baterías.
307. Para la prestación del servicio de monitoreo y gestión de UPS a través de SNMP, el ICBF garantizará en cada una de las sedes un punto de red para la conexión de las UPS al igual que un agente SNMP para las UPS que serán monitoreadas.

Nota: La solución ofrecida para el servicio de monitoreo y administración centralizada no puede generar costos adicionales en cuanto a conectividad. Lo anterior teniendo en cuenta que se utilizarán los enlaces WAN y LAN de la Entidad. Si la sede en la cual se encuentra la UPS monitoreable no cuenta con conectividad (canal dedicado de comunicaciones), se excluirá del servicio de monitoreo SNMP.

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

308. Para la prestación del servicio de monitoreo y gestión de UPS a través de SNMP, el ICBF garantizará en cada una de las sedes un punto de red para la conexión de las UPS al igual que un agente SNMP para las UPS que serán monitoreadas.
309. Reportar a través de la herramienta de Gestión de forma automática (Mesa de Servicio) los incidentes o novedades del servicio para que el administrador de Ups o persona delegada por el ICBF proceda a la revisión pertinente.

Backup

310. EL CONTRATISTA administrará la herramienta de Backup Networker de EMC que tiene el ICBF licenciada, con sus correspondientes módulos , para realizar las copias de seguridad de todas las aplicaciones, sistemas operativos de servidor, bases de datos, correo electrónico, repositorios de información y plataforma de virtualización. En caso de requerirse licenciamiento de la herramienta de Backup Networker adicional a la actualmente en posesión del ICBF, el ICBF proveerá este licenciamiento, previo estudio de dimensionamiento en conjunto con EL CONTRATISTA.
311. EL CONTRATISTA deberá considerar la intercomunicación entre la herramienta de respaldos EMC Networker y la herramienta de gestión, de manera tal que de forma automática se generen tickets ante el fallo en la realización de una tarea de respaldo y/o restauración. Esto deberá permitir la realización de informes que permitan determinar el cumplimiento de ANS para su evaluación y revisión mensual.

Nota: Si EL CONTRATISTA decide utilizar otras herramientas para la realización y restauración de backups, deberá considerar el debido licenciamiento y garantizar la compatibilidad con los backups históricos, realizados con Netowrker y los medios magnéticos utilizados, deben ser Cintas LTO4. Asimismo, deberá evaluarse el reporte automático entre la Solución de Backup y la herramienta de gestión de servicios.

Almacenamiento

312. EL CONTRATISTA deberá administrar las herramientas:
- Unisphere
- Navisphere
- Analyser EMC
- Thin Provisioning EMC
- SAN Copy EMC
- SnapView EMC
- Fast Suite EMC.

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

Las cuales deberán ser administradas, configuradas, monitoreadas y gestionadas por EL CONTRATISTA, así mismo proveer el personal especializado que estime conveniente para la gestión de las mismas de acuerdo al Anexo 006 - PERFILES-PROFESIONALES REQUERIDOS.

Seguridad

313. EL CONTRATISTA debe suministrar y administrar herramientas de monitoreo para los firewall de seguridad perimetral, la cual debe estar integrada directamente a la herramienta de la Mesa de Servicio para facilitar labores de correlación de eventos y permitir gestión y administración centralizada, además debe generar automáticamente tickets en tiempo real.

314. EL CONTRATISTA debe disponer la herramienta de monitoreo requerida para medir la disponibilidad del servicio de firewall durante cada periodo de operación con el fin de que el ICBF pueda determinar la aplicación o no del ANS Asociado.

315. EL CONTRATISTA debe administrar la solución de antivirus actual y su infraestructura. Actualmente se cuenta con Microsoft System Center Endpoint Protection. En caso de cambiar la solución de antivirus durante la vigencia del contrato, EL CONTRATISTA deberá asumir la instalación, configuración, despliegue y administración de la nueva solución, así como todas las labores requeridas para la transición hacia ella.

7.2. Obligaciones Generales

316. Mantener, gestionar, administrar, renovar, configurar y actualizar los nombres de dominio públicos del ICBF y los servicios que de él se desprendan y adquirir otros que resulten necesarios durante la vigencia del contrato.

317. Prestar los servicios con personal calificado, especializado que cumpla con los perfiles y experiencia exigidos por el ICBF como se indica en el o Anexo 006 - PERFILES-PROFESIONALES REQUERIDOS.

318. Diseñar, entregar y aplicar los formatos, procesos y procedimientos para la prestación del servicio con el detalle que el ICBF lo exija.

319. Mantener actualizado el inventario e información de la infraestructura tecnológica con el detalle que exija el ICBF. Para ello el ICBF podrá solicitar los reportes con la periodicidad y el detalle que lo considere necesario.

320. Será responsabilidad de EL CONTRATISTA el mantener actualizado el inventario de la infraestructura administrada, la cual deberá ser reportada al ICBF. EL CONTRATISTA deberá realizar un inventario en sitio como mínimo al inicio del contrato y al finalizar el mismo, y una vez al año incluyendo equipos que no estén conectados dentro de la red del instituto (Ej. Equipos en Bodega).

321. Diseñar, documentar e implementar (previa aprobación del ICBF) planes de contingencia y continuidad para todos los servicios objeto del presente proceso, ante cualquier eventualidad que afecte la continuidad en la operación de los mismos.

322. Para el caso de renuncias, incapacidades, licencias, vacaciones, traslados de personal o cambios de personal a solicitud del ICBF, EL CONTRATISTA debe incluir un proceso de empalme y transferencia de conocimiento de mínimo una semana. Para este fin EL CONTRATISTA deberá entregar un documento al inicio del contrato donde se especifique el proceso que se debe llevar para realizar el empalme.

323. Presentar semanalmente el cronograma de disponibilidad del personal de EL CONTRATISTA asignado al proyecto.

324. Presentar notificación con 15 días de anticipación, cuando se planee retirar o reemplazar a cualquier miembro del equipo, explicando el motivo del retiro y el plan de trabajo para reemplazarlo.

325. EL CONTRATISTA deberá realizar un plan de trabajo para la implementación de las políticas y recomendaciones que genere el Sistema de Gestión de Seguridad de la Información (SGSI) del ICBF, y realizar su ejecución.

326. Facilitar al ICBF el acceso a todas las herramientas y consolas de gestión y administración de los servicios, con acceso en modo de lectura, mediante la creación de las cuentas a que haya lugar o la habilitación de los privilegios sobre las cuentas de Directorio Activo que el ICBF designe, configurándolas adecuadamente para tal tipo de acceso.

327. Notificar, justificar y proponer de manera inmediata al ICBF cualquier cambio que considere necesario o aconsejable realizar sobre cualquiera de los servicios que le fueron dados a administrar para optimizar su operación y someterlo a Control de Cambios si fuese necesario.

328. Documentar detalladamente los procedimientos, instructivos e instrumentos técnicos a utilizar durante los cambios que se requieran sobre cualquiera de los

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

servicios para su optimización, tanto para la presentación de la solicitud del cambio como para la generación de conocimiento, documentos que deben ser aprobados por el ICBF.

329. Garantizar el correcto funcionamiento de todos los servicios contratados, comprometiéndose a subsanar las fallas que le sean atribuibles durante la vigencia del contrato. (demostrable con los demás operadores de tecnología para ICBF).

330. Garantizar la operación en los servicios bajo los horarios, tiempos de respuesta y condiciones establecidas en el presente Anexo Técnico.

331. Garantizar al ICBF que cumple y conoce la normatividad, reglas y lineamientos técnicos y legales para la prestación de la operación y los servicios contratados.

332. Garantizar al ICBF que cuenta con las condiciones mínimas de seguridad para todos los procesos, establecidas en los estándares internacionales y en aquellas incluidas en el presente Anexo Técnico.

333. Garantizar que tiene establecidos los controles de calidad sobre los servicios contratados.

334. Garantizar los viáticos y herramientas necesarios para el desplazamiento de su personal de soporte a los sitios del ICBF a Nivel Nacional de acuerdo al alcance descrito en el presente documento.

335. Cumplir y dar a conocer a sus colaboradores las políticas, procedimientos, normas y responsabilidades en materia de seguridad definidas por el ICBF.

336. Licenciar todo el software que provea y disponga para dar cumplimento al objeto del contrato.

337. Monitorear y administrar el desempeño de toda la infraestructura de tecnología informática expuestos en este documento para el ICBF.

338. Realizar el plan de ampliaciones y mejora de la plataforma tecnológica del ICBF para los próximos 4 años, el cual deberá ser construido en conjunto con el ICBF durante los 8 (ocho) primeros meses de ejecución del contrato.

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

339. Garantizar la protección y seguridad de los datos, programas, aplicaciones, bases de datos, infraestructura e información del ICBF velando por cumplir con los tres pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

340. Realizar en conjunto con el ICBF los procedimientos para llevar a cabo la instalación de aplicativos y bases de datos o cualquier otro software en los equipos al servicio del ICBF.

341. Realizar el acompañamiento para la creación y/o revisión, implementación y divulgación de las políticas de seguridad y de control informática establecidas por el ICBF.

342. Reportar por escrito al ICBF cualquier sugerencia que contribuya a la obtención de mejores resultados.

343. Acatar las instrucciones que imparta el ICBF para el cabal cumplimiento del contrato, a través del Supervisor del contrato.

344. 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.

345. 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.

346. 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), del personal que hace parte del contrato, para efectos del pago.

347. 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.

348. Cumplir con las obligaciones derivadas del contrato actuando con alto grado de profesionalismo responsabilidad y eficacia en la ejecución de las tareas correspondientes.

349. 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.

350. Suscribir el acta de liquidación del contrato.

351. 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.

352. Mantener monitoreados los servicios 7x24x365, durante la duración del contrato.

353. Trabajar, en conjunto con la SRT en la gestión para el tratamiento y cierre de acciones preventivas, correctivas o de mejora, relacionada con el servicio, y que estén alineadas con el Sistema de Gestión de Calidad del ICBF, o los casos activos en herramienta de gestión de Mesa de Servicio.

354. Presentar informes mensuales de gestión (por servicio) que reflejen el desempeño en la ejecución de los servicios, resaltando la medición de los ANS, así como el análisis de las actividades realizadas, planeadas, suspendidas, incumplidas, los controles de cambios, reportes de niveles de utilización, incluyendo como mínimo crecimiento mensual, incidentes, análisis de errores, alertas y las sugerencias y recomendaciones que deban ser puestas a consideración del ICBF, entre otros que deberá ser acordados. Los informes deben entregarse a acada uno de los líderes de los servicios del ICBF en los primeros 5 días habiles del mes.

355. Llevar el registro de los controles de cambios para las actividades que afecten los ambientes administrados.

356. Elaborar la documentación requerida para la presentación de solicitudes de cambio ante el Comité de Control de Cambios de la entidad, de acuerdo a los procedimientos definidos en tal sentido.

357. Apoyar a la SRT en el diseño, implementación, medición y administración de pruebas piloto relacionadas con los servicios, contratadas a través de este contrato u otros inclusive sin que esto genere un costo adicional para ambas partes.

358. Apoyar a la SRT en la generación de conocimiento relacionado con los servicios, para su uso y registro en la base de datos de conocimientos de TI del ICBF, así como

en la generación de propuestas sobre nuevos ANS o acciones que repercutan en la mejora de los servicios.

359. Apoyar en la implementación de soluciones nuevas relacionadas con los servicios, adquiridas a través de este contrato u otros inclusive.

360. Proponer recomendaciones y acciones de mejora que sobre los servicios, basado en las nuevas tendencias tecnológicas, planes de capacidad y consulta a expertos realizadas.

361. EL CONTRATISTA debe designar personal especializado que se encuentre disponible de forma permanente (7x24) para responder a las alertas y/o incidentes generados en la plataforma tecnológica.

362. Desarrollar un plan de capacidad como mínimo una vez al año, donde se evalúe el planteamiento de la suficiencia de la infraestructura del ICBF, así como la pertinencia de realizar nuevas adquisiciones o mejoras.

363. Acoger las recomendaciones que durante la vigencia del contrato realice la SRT, las cuales contribuyan en la mejora de prestación del servicio.

364. Ejecutar actividades programadas y no programadas propias sobre la infraestructura y los servicios.

365. Debe diseñar, elaborar, actualizar y documentar el plan de contingencia, el cual deberá presentarse al ICBF para su estudio y aprobación dentro del segundo trimestre de la ejecución del contrato.

366. Generar y ejecutar de forma anual el cronograma de las actividades de mantenimiento con fechas y responsables para la infraestructura y los servicios.

367. EL CONTRATISTA deberá brindar apoyo y proponer activamente recomendaciones al ICBF tendientes a optimizar el uso de recursos, asegurar la disponibilidad, seguridad, seguimiento, control, continuidad, operación y buen desempeño de la infraestructura del ICBF. Este apoyo derivará en planes de acción donde se detallen los requerimientos y actividades necesarias para aplicar dichas recomendaciones.

368. Notificar al ICBF cualquier incidente, anomalía o alerta que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible

según la hora de aparición del incidente, y actuar proactivamente en la búsqueda y aplicación de la solución, con el objetivo de minimizar el impacto.

369. Diseñar, crear, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos de los servicios.

370. Dar respuesta a las consultas técnicas realizadas por el ICBF, asesorando en el mejoramiento y optimización de recursos, con el fin de garantizar la disponibilidad y buen desempeño de la infraestructura.

371. Preparar la información solicitada por el ICBF dentro de un plazo máximo de 24 horas hábiles siguientes al requerimiento, en su defecto deberá entregar dentro de este mismo plazo una respuesta que incluya sustentadamente, la razón por la cual no es posible entregar la información en el tiempo establecido y la descripción o plan de trabajo con la fecha de entrega de la información, la cual no podrá ser superior en ningún caso a 5 días hábiles.

372. EL CONTRATISTA deberá disponer de un especialista por servicio, el cual estará en constante comunicación con el líder del respectivo servicio designado por el ICBF.

373. EL CONTRATISTA deberá garantizar que la incorporación y/o sustitución de alguno de los especialistas, sea informado con antelación al ICBF y este debe cumplir con el Anexo 006 - PERFILES-PROFESIONALES REQUERIDOS.

374. La disponibilidad de todos los recursos de personal asignados por parte de EL CONTRATISTA a este contrato, serán permanentes, sin que las posibles incidencias relacionadas afecten al ICBF. En este sentido, será responsabilidad exclusiva de EL CONTRATISTA que no exista ningún periodo de carencia entre la baja de un recurso de cualquier perfil y la reposición del mismo. La incorporación, sustitución, compensatorios o baja de cualquier especialista designado por EL CONTRATISTA, debe ser informado al ICBF con 8 días de antelación.

375. EL CONTRATISTA deberá informar al ICBF los compensatorios de los especialistas semanalmente.

376. Será responsabilidad de EL CONTRATISTA la formación de su personal, en cuanto a la realización de todos los cursos que se consideren necesarios e imprescindibles, incluyendo los de actualización, para la correcta prestación del 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

377. EL CONTRATISTA no debe contemplar un Data Center diferente para la replicación, sin embargo debe contar con el modelo de IaaS.

378. Generar, documentar, validar, aprobar y asesorar los controles de cambio que se presenten relacionados a los servicios, dimensionando las ventanas de mantenimiento, tiempos de indisponibilidad, planes de contingencia, rollback, identificación y mitigación de los posibles riesgos, de acuerdo a los procedimientos ya establecidos por el comité de control de cambios del ICBF.

379. Garantizar al ICBF la confidencialidad y accesos a la información, para esto se compromete a firmar y cumplir el acuerdo de confidencialidad.

380. Optimizar los procedimientos de operación y procesamiento de la plataforma, teniendo en cuenta las políticas y procedimientos establecidos por el ICBF para manejo de cambios e incidentes.

381. EL CONTRATISTA deberá analizar, proponer y documentar mejoras sobre la infraestructura tecnológica del ICBF.

382. EL CONTRATISTA deberá ejecutar cualquier tipo de actualización y mejora sobre la infraestructura, sin que esto genere costos adicionales a la entidad. El ICBF suministrara los recursos de hardware y licenciamiento necesarios para tal fin.

383. Realizar el cruce y la actualización de los usuarios en cada uno de los servicios versus Directorio Activo cada quince (15) días. EL CONTRATISTA debe garantizar que los usuarios desactivados, eliminados e inactivos no tengan ningún tipo de acceso a los servicios del ICBF.

384. EL CONTRATISTA deberá realizar la gestión con terceros de incidentes y requerimientos que así lo requieran, previa autorización del ICBF.

385. El CONTRATISTA deberá suministrar, administrar o configurar en caso de ser necesario, las herramientas de Gestión para los servicios contratados, así como las herramientas de monitoreo y diagnostico que permitan gestionar, registrar, monitorear, controlar, alertar y generar reportes de cada servicio requerido con el fin garantizar la óptima prestación de los mismos.

386. EL CONTRATISTA debe suministrar repuestos para los equipos propiedad del ICBF que no se encuentren cubiertos por garantías o la pierdan durante la vigencia del

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

Contrato de Outsourcing. Equipos relacionados en el ANEXO 010 - INVENTARIO EQUIPOS DATA CENTER EXTERNO.

7.3. Obligaciones del Sistema Integrado de Gestión:

7.3.1. Para el eje de Calidad

7.3.1.1. El operador/contratista debe referir el diseño e implementación de un procedimiento de personal idóneo y competente para el desarrollo de los servicios a contratar.

7.3.1.2. El operador/contratista debe socializar con el equipo que realizará las actividades definidas en el contrato, la información básica del ICBF (Misión, Visión, Principios, Objetivos Estratégicos y Políticas de los Sistemas de Gestión).

7.3.2. Para el eje de Seguridad y Salud Ocupacional

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

7.3.2.1. El operador/contratista debe referir el diseño e implementación de un Plan Básico de Seguridad y Salud Ocupacional para el equipo que realizará las actividades definidas en el contrato.

7.3.2.2. Cuando el operador/contratista lidere la realización de eventos en representación del ICBF y con la participación de 35 personas o más debe tener en cuenta las recomendaciones impartidas por la Entidad en la cartilla de Buenas Prácticas de Seguridad.

7.3.2.3. Todo el personal del contratista deberá estar afiliado al Sistema de Seguridad Social en riesgos laborales.

7.3.2.4. Antes de iniciar cualquier actividad en el ICBF todos los trabajadores del contratista deben recibir inducción en Seguridad y Salud en el trabajo.

7.3.2.5. Suministrar a sus trabajadores todos los Elementos de Protección Personal requeridos para la realización de sus actividades y garantizar el uso correcto de estos durante la ejecución de los trabajos. En caso de deterioro o daño el remplazo deberá hacerse de forma inmediata.

7.3.2.6. Presentar al ICBF la matriz de riesgos ocupacionales, un plan para su control y los procedimientos de seguridad y salud ocupacional, en el que se definan objetivos y se tracen metas de acuerdo a la identificación de peligros.

7.3.2.7. Durante la ejecución del contrato el contratista deberá cumplir con las normas reglamentarias sobre seguridad y salud en el trabajo, medicina preventiva, higiene y seguridad industrial y los demás aspectos inherentes que han sido establecidos o establezca la ley y los organismos de control.

7.3.2.8. Es responsabilidad del contratista garantizar las condiciones de seguridad de su personal, así como de los equipos propios o de la empresa; para esto deberá disponer de procedimientos estandarizados para las actividades de alto riesgo y garantizar mecanismos verificables de control operativo.

7.3.2.9. El ICBF podrá suspender trabajos del contratista si éstos no se ajustan a los estándares de seguridad establecidos por normas técnicas nacionales o internacionales o a la normatividad legal.

7.3.2.10. EL contratista es responsable del reporte a la ARL y EPS, atención en salud e investigación de los incidentes y accidentes de trabajo presentados durante el desarrollo de las actividades objeto del contrato

7.3.3. Para el eje Ambiental

7.3.3.1. El operador/contratista, de acuerdo a la actividad a desarrollar debe establecer el análisis de los aspectos e impactos ambientales asociados al contrato que vaya a ejecutar, establecer las acciones tendientes a reducir, mitigar y corregir los impactos ambientales significativos.

7.3.3.2. Para los contratos de mantenimiento de infraestructura, el contratista debe conocer la legislación ambiental aplicable y establecer las acciones de cumplimiento de las mismas.

7.3.3.3. El contratista cuyo objeto vincule la supervisión e interventoría a operadores/contratistas (misionales/funcionales), deben tener presente los aspectos e impactos ambientales, los requisitos legales regionales y locales asociados a la actividad a desarrollar, los estándares de supervisión y seguimiento.

7.3.4. 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:

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

7.3.4.1. El operador/contratista debe garantizar los procesos adecuados para la protección y confidencialidad de la información suministrada por los beneficiarios.

7.3.5. Para el eje de Innovación

7.3.5.1. El Operador/contratista deberá promover y desarrollar acciones de innovación y mejora que permitan ajustar y fortalecer el trabajo a desarrollar con los beneficiarios.

8 LUGAR DE EJECUCIÓN DEL CONTRATO

Durante la vigencia del contrato, los servicios se prestarán en la Sede de la Dirección General, Sede de la Calle 57, Regionales, Data Center Externo proveído por EL CONTRATISTA y con los alcances que se especifican en este documento para cada uno de los servicios.

EL CONTRATISTA deberá garantizar la presencia física de los especialistas encargados de los servicios objeto de este contrato cuando el ICBF lo requiera en sus instalaciones.

9 PLAZO DE EJECUCIÓN

La duración del contrato será de 10 meses y 15 días, contados a partir de la legalización del contrato.

10 FORMA DE PAGO DEL VALOR DEL CONTRATO

El valor del contrato a suscribir será hasta por el valor del 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.

Facturación:

EL CONTRATISTA deberá facturar los servicios efectivamente prestados de acuerdo con los ítems definidos en la propuesta económica, y realizando los descuentos correspondientes por ANS aplicables en el periodo facturado.

Anticipo:

El ICBF entregará a El Contratista un anticipo que será definido con el resultado del estudio de mercado.

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 valor del anticipo que se entregará a EL CONTRATISTA, deberá ser amortizado en los 3 primeros meses de la etapa de operación, ya que en la etapa de Transición no se pagará ningún servicio.

Forma de pago:
Los servicios se pagarán de acuerdo con las siguientes consideraciones, sin perjuicio de los descuentos por ANS a que haya lugar:

- **Servidores**

Se realizarán pagos mensuales a EL CONTRATISTA por número de servidores (Físicos y Virtuales) administrados según el informe de gestión de servidores de la línea base en el periodo facturado.

- **Controlador de Dominio**

Se pagará a EL CONTRATISTA un valor fijo mensual por la administración del servicio de DHCP, DNS, DA y Entidades Certificadoras.

- **Aplicaciones**

Se realizarán pagos mensuales a EL CONTRATISTA por el número de aplicaciones administradas según el informe de gestión de aplicaciones en línea base en el periodo facturado.

- **Base de datos**

Se realizarán pagos mensuales a EL CONTRATISTA por número de base de datos administradas según el informe de gestión de base de datos en línea base en el periodo facturado.

- **Backups**

Para el servicio de administración de respaldo y restauración de la información se pagará a EL CONTRATISTA un valor fijo mensual por la operación y administración del servicio de Backup y las herramientas para el dispuesto.

Para el servicio de contratación de renovación de soporte 7x24 de las soluciones de respaldo, se pagará a EL CONTRATISTA de forma mensual en cuotas iguales el valor ofertado, dividido en el número de meses de la ETAPA DE OPERACIÓN a partir del mes de mayo de 2015. El contrato de soporte actual 7x24 sobre la solución de respaldo en disco EMC AVAMAR finaliza el 30 de abril de 2015.

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

Para el servicio de custodia de medios, se pagará a EL CONTRATISTA un valor fijo mensual por este concepto, independientemente la cantidad de medios en custodia que se resguarden.

En el caso de que se opte por tomar los servicios de migración de respaldos históricos a una solución distinta a la que actualmente tiene el ICBF, se pagará a EL CONTRATISTA mensualmente por TB migrado en el período facturado, lo cual será validado en el informe de Gestión mensual respectivo.

- **Almacenamiento NAS y SAN.**

Se pagará a EL CONTRATISTA un valor fijo mensual por la operación y administración del servicio de Almacenamiento según informe mensual.

Para el servicio de contratación de renovación de soporte 7x24 de las soluciones de almacenamiento SAN y NAS, se pagará a EL CONTRATISTA de forma mensual en cuotas iguales el valor ofertado, dividido en el número de meses de la ETAPA DE OPERACIÓN a partir del mes de abril de 2015. El contrato de soporte actual 7x24 sobre las soluciones de almacenamiento finaliza el 23 de marzo de 2015.

- **Centro de Cómputo**

Para el servicio de Centro de Cómputo (Sede de la Dirección General ICBF) se pagará a EL CONTRATISTA un valor mensual fijo por concepto de administración, previa presentación y verificación del informe de gestión de Centro de Cómputo del periodo facturado.

- **Office 365.**

Se pagará a EL CONTRATISTA un valor fijo mensual por la administración y soporte de los servicios que componen Office 365 que deberán estas discriminados de la siguiente forma:

- Servicios de Administración de Federación y Entorno Hibrido
- Administración de Plataforma Hibrida Office 365 (Consolas de Administración On-Line / On-Premise)
- Correo Electrónico (On-Line / On-Premise)
- Lync (On-Line / On-Premise)
- Sharepoint (On-Line / On-Premise)

- **Herramientas de Gestión y Monitoreo**

Por la Implementación System Center Operations Manager, se pagará a EL CONTRATISTA una sola vez un valor fijo global correspondiente a todas las actividades necesarias para la implementación, previa aceptación por parte del supervisor del contrato.

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

Se pagará a EL CONTRATISTA de manera mensual:

- Monitoreo y Administración de la Infraestructura Tecnológica del ICBF y Servicios expuesto en el numeral 6.10 (Servidores, Equipos, Bases de Datos, Almacenamiento, Aplicaciones, Equipos Activos de Red, UPS, Aires Acondicionados, Entre otros) a través de la Operación, Administración y Mantenimiento de las herramientas que están actualmente implementadas en el ICBF.

- Suministro de herramienta(s) en caso de que las herramientas del ICBF de forma comprobada técnicamente no cumplan algún requerimiento que se solicite en el numeral 6.10.

  Para el presente estudio de mercado y a partir del resultado de este, la entidad escogerá una de las siguientes 2 opciones:

  - OPCIÓN 1: Pago por uso del servicio de las herramientas durante el tiempo de ejecución del presente contrato.

  - OPCIÓN 2: Licenciamiento a perpetuidad de las herramientas que utilice EL CONTRATISTA en caso de ser necesario.

- Administración y monitoreo de Licenciamiento

- **Telefonía IP**

Se pagará un valor mensual fijo por el servicio de Telefonía IP previa verificación y aprobación del informe de gestión.

- **Seguridad**

Se pagará un valor mensual fijo por cada servicio de manera independiente, de los servicios que componen la solución de seguridad informática descrita en este documento. Los servicios son:

- Seguridad Perimetral
- Seguridad Avanzada de Red
- Seguridad de Acceso a la red
- Seguridad en Aplicaciones WEB
- Seguridad en Bases de Datos
- Logs y Reportes
- Servicio de Security Information Event Management (SIEM)

El pago se realizará posterior a la verificación y aprobación del informe de gestión.

- **Organización del proyecto:**

Se pagará un valor mensual por la gestión y administración del proyecto.

Calculo de los ANS:

El valor máximo a pagar por el servicio se establecerá teniendo en cuenta la unidad de medida del servicio y la tarifa establecida en la propuesta económica para el servicio a liquidar.
La liquidación mensual de cada servicio se realizará con base en la siguiente fórmula

$$Valor\ Servicio\ i = \sum_{s=1}^{Número\ de\ ANS\ para\ el\ servicio\ i} Valor\ ANS\ s * FC\ ANSs$$

Donde,

Servicio i	Servicio objeto de liquidación
Valor ANS s	Valor mensual del servicio i * Porcentaje de ponderación ANS s
ANS s	Acuerdos de nivel de servicio del Servicio i
FC ANS s	Factor de conformidad del ANS s del servicio i

Factor de conformidad = 100% - % de descuento a aplicar sobre el valor mensual del servicio i, de acuerdo con el cumplimento del ANS s y la “Tabla de descuento aplicado” establecida para el ANS s.

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.

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

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

En caso de estimarse costos adicionales de implementación, configuración, administración y operación de cualquier herramienta, servicio o plataforma propiedad del ICBF, los mismos serán sometidos a negociación con el ICBF primando siempre el costo promedio de 3 cotizaciones del mercado realizadas por el ICBF.

11 ANEXOS

- Anexo 001 - TABLA LINEAS BASE.xlsx
- Anexo 002 - ACUERDOS DE NIVELES DE SERVICIO.xlsx
- Anexo 003 - ETAPAS DEL PROYECTO.xlsx
- Anexo 004 - CONSIDERACIONES ETAPA TRANSICION.xlsx
- Anexo 005 - MATRIZ CHEQUEO ORGANIZACION PROYECTO.xlsx
- Anexo 006 - PERFILES PROFESIONALES REQUERIDOS.xlsx
- Anexo 007 - REPORTES OPERACIÓN.xlsx
- Anexo 008 - PLATAFORMA DE TELEFONÍA IP.docx
- Anexo 009 - EQUIPOS DE TELEFONÍA IP POR SEDE.xlsx

12 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
John Lizcano Castro **Líder Grupo Acceso a Datos**	**Luis Felipe Onofre** **Subdirección de Recursos Informáticos**	**Hernan Hoyos** **Director de Información y Tecnología**

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