

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

Fecha 29/09/2015

### 1. DENOMINACIÓN DEL BIEN O SERVICIO

Servicios de Tecnología de la Información y Comunicaciones (TIC) bajo la modalidad de Outsourcing para la administración de la Infraestructura Tecnológica de la Entidad, incluidas las actividades de administración, gestión, monitoreo y control especializado de la plataforma de Almacenamiento, Respaldo, Servidores, Aplicaciones, Bases de Datos, Office 365, Seguridad Informática, Redes LAN y Redes Inalámbricas, Correo Electrónico, servicio de Internet Móvil, servicios 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

El ICBF requiere la administración, gestión y monitoreo de las soluciones de Correo Electrónico, Almacenamiento, Respaldo, Servidores, Aplicaciones, Bases de Datos, Office 365, servicios Tecnológicos con los que cuenta el ICBF actualmente para brindar los servicios misionales a los beneficiarios de la Entidad. Adicionalmente requiere la administración de la Red LAN y Red Inalámbricas (WLAN) de la Sede de la Dirección General y Sedes anexas y la administración del Centro de Computo ubicado en la Sede de Dirección General en el cual residen los equipos que

dan conectividad a esta sede y por ende acceso a los aplicativos, bases de datos y demás servicios requeridos por las áreas misionales y de apoyo de la sede mencionada.

De otra parte, el ICBF requiere el Servicio de monitoreo (SOC - Security Operation Center) para una Gestión integrada de seguridad, operaciones y riesgos de TI en la plataforma tecnológica instalada en el ICBF y el suministro de una solución de Seguridad Perimetral para garantizar la confidencialidad, integridad y disponibilidad de la información, evitando y dando tratamientos a distintas amenazas referentes a la seguridad informática y el servicio de Internet Móvil.

Los servicios descritos anteriormente, al igual que sus valores agregados y conexos serán contratados bajo la modalidad de Outsourcing.

#### 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.

#### MARCOS DE REFERENCIA

- ISO/IEC 27001, estándar para Sistemas de Gestión de Seguridad de la Información
- ISO/IEC 20000, estándar para la Gestión de TI
- ITIL, marco de referencia para la gestión de TI
- COBIT, marco de referencia para el Gobierno de TI
- PMI, marco de referencia para la gestión de proyectos
- OSSTMM, (Manual de la Metodología Abierta de Testeo de Seguridad)

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

##### 6.1 INTRODUCCIÓN

EL ICBF requiere que El Contratista suministre los servicios sobre la infraestructura propia de la Entidad, en los sitios (sedes) que se enuncian en el presente documento donde hace presencia el ICBF, partiendo de una línea base ANEXO 001-LINEA BASE-INFRAESTRUCTURA y ajustándose a los cambios que se den en ésta, según la dinámica de las necesidades institucionales.

La prestación de los servicios por parte del Contratista 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 20000 e ISO 9001 en su última versión vigente.

La ejecución del contrato y el cumplimiento de las actividades y obligaciones contractuales se llevarán a cabo en tres diferentes etapas, las cuales se describen en el presente documento, durante las cuales El Contratista las tendrá a su cargo.

La estrategia para la prestación de los servicios de infraestructura y la calidad del servicio del Contratista, deberá contemplar los Acuerdos de Niveles de Servicios (ANS) definidos para cada uno de los servicios en 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 mencionado, 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 por el ICBF en la revisión mensual de los informes de gestión presentados para cada uno de los servicios por parte del Contratista.

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.

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 ubicada en Bogotá en la Av cra 68 No. 64 c - 75 en donde se encuentra el Centro de Cómputo y desde las instalaciones de la empresa IFX Networks SAS ubicado en la Carrera 69 No. 25B – 44 oficina 815 Edificio WBP donde se encuentra un Data Center TIER III de igual manera en las instalaciones del ICBF ubicadas en Bogotá en la Calle 57 No. 16 – 35 se encuentran la Dirección de Información y Tecnología (DIT), la Subdirección de Recursos Tecnológicos (SRT) 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 ubicadas a 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 otra parte, el personal del CONTRATISTA es el responsable de realizar la instalación, administración, operación, mantenimiento, monitoreo y soporte de toda la plataforma tecnológica del ICBF, tanto propia, como arrendada, de acuerdo con lo expuesto en el presente documento.

## **6.2 CONSIDERACIONES GENERALES**

El ICBF requiere que El Contratista adopte las mejores prácticas de ITIL (como mínimo v3), para la gestión del servicio y acompañe al ICBF en los procesos de implementación, actualización y sensibilización de las gestiones durante todas las etapas del contrato. Así mismo, deberá elaborar e implementar los procesos de gestión necesarios para la entrega y soporte de los servicios, previa aprobación por parte del ICBF.

Durante el tiempo de ejecución 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 Capacidad.
- Gestor de Niveles de Servicio.
- Gestor de Continuidad.
- Gestor de Disponibilidad.
- Gestor de Riesgos.
- Gestor de Incidentes
- Gestor de Problemas
- Gestor de Seguridad
- **Gestor de Requerimientos**

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:

- Las especificaciones técnicas de este documento.
- Anexos Informativos:
  - Anexo 001 - LINEA BASE-INFRAESTRUCTURA.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 - EQUIPOS - RED LAN –WLAN
  - Anexo 009 - INVENTARIO EQUIPOS DATACENTER EXTERNO
  - Anexo 010 – BACKUP
  - Anexo 011 - EQUIPOS DE TELEFONÍA IP POR SEDE.
  - Anexo 012 - SERVIDORES EN CLOUD

Los Acuerdos de Nivel de Servicio (ANS) serán los descritos en el documento **Anexo 002 - Acuerdos de Niveles de Servicio**, EL ICBF requiere que El Contratista garantice la correcta implementación, configuración, administración y seguimiento en las Herramientas de Monitoreo, Seguridad y/o Gestión necesarias para su medición, adicionalmente, certificar la no manipulación de los resultados, el acceso, la verificación y validación de los mismos.

Con el objeto de que el ICBF pueda realizar los respectivos seguimientos y las penalizaciones a que haya lugar, se requiere que El Contratista genere un informe de ANS mensual para cada uno de los servicios, dado que a partir de la verificación de este informe y mediante las herramientas de monitoreo, seguridad y/o gestión se realizaran los seguimientos mensuales.

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 - LINEA BASE - INFRAESTRUCTURA.

#### 6.2.1 Dinámica para el cambio de los ANS y Línea Base de los Servicios:

Con el fin de mantener la calidad en la operación de los servicios de TI del ICBF, se contempla durante la etapa de operación la revisión trimesral de ANS y la revisión trimestral de la Línea Base

de los servicios; esta revisión se realizará a través de los Comité Operativo y Ejecutivo respectivamente, 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. **Cuando se presente una modificación o inclusión de un ANS este tendrá dos (2) meses de estabilización, periodo durante el cual no presentarán penalización.**

### 6.2.2 Otras Consideraciones:

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.

El ICBF podrá:

- Solicitar en cualquier momento el cambio de cualquier miembro del equipo de trabajo del Contratista cuando se presenten deficiencias técnicas, profesionales y de actitud en la prestación del servicio o labor a su cargo. De acuerdo con los requerimientos, exigencias y necesidades del ICBF.
- Solicitar las hojas de vida para verificar las competencias y calidad del personal de El Contratista.
- Considerar a todos los terceros, aliados y socios de negocio del Contratista, que participen en la prestación de servicios objeto del presente documento, como personal del Contratista, por lo cual El Contratista será el único responsable de lo que realicen estos terceros.

El ICBF suscribió en el año 2014 el contrato 1343 con la Unión Temporal Gestion Integral Mesa ICBF hasta el 31 de julio de 2018, el cual suministra los servicios de mesa de servicio y soporte en sitio. Dentro de este contrato el proveedor dispone el servicio de herramienta de Gestión Help People, a través de la cual se gestionan los tickets de incidentes, requerimientos y controles de cambios y soporta la base de conocimiento y el catálogo de servicio.

### 6.3 ALCANCE

El alcance del contrato se resume en los servicios relacionados a continuación, que debe proveer El Contratista a nivel nacional, de acuerdo con lo detallado en el presente documento y anexos:

- Centros de Cómputo (Sede de la Dirección General)
- Servidores

- Almacenamiento
- Respaldo
- Aplicaciones
- Bases de Datos
- Seguridad Informática
- Correo Electrónico
- Servicio de Gestión y Monitoreo
- Office 365
- Red Lan
- Red Wlan
- Internet y Telefonía Móvil

A fin de implementar los servicios, El Contratista debe contemplar con carácter obligatorio los requerimientos establecidos por parte del ICBF en el presente 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.

**Nota 1:** 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 y por servicios no prestados. El procedimiento para proveer y pagar los servicios adicionales es el siguiente:

- Presentar la solicitud en los comités operativos con el fin de validar y justificar la ejecución del servicio y validar la forma de pago.
- Solicitud de cotización por parte del supervisor del contrato al Contratista, acompañada de las especificaciones técnicas del servicio a contratar y sus ANS, si aplica.
- La cotización allegada por El Contratista deberá estar acorde a los precios del mercado y los tiempos exigidos por el ICBF. El ICBF podrá realizar la validación de la cotización presentada por El Contratista, solicitando al mercado cotizaciones adicionales.
- La entrega del servicio para puesta en funcionamiento se realizará mediante un acta por parte del supervisor del contrato, previa confirmación de cumplimiento integral de las condiciones técnicas solicitadas.

#### 6.4 ETAPAS

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

El detalle de cada etapa y sus entregables se encuentra en el *Anexo 003 - Etapas Del Proyecto*, donde se encuentran descritos los entregables que El Contratista debe realizar en cada una de las etapas, para revisión y aprobación por parte del supervisor del Contrato.

#### **6.4.1 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, en cuanto a todos los servicios e instalaciones requeridas para la continuidad en la operación. El Contratista tendrá el acompañamiento del operador actual de TI y del ICBF para realizar el empalme para la migración de servicios, soluciones y ejecución de pruebas necesarias en el 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 de los mismos.

Esta etapa está distribuida en fases las cuales se definen en el *Anexo 003 - Etapas Del Proyecto* y en Anexo 004 - CONSIDERACIONES ETAPA TRANSICION.

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 del Contratista por causas imputables al mismo, el ICBF descontará de las facturas de la ETAPA DE OPERACIÓN el 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 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.

#### **6.4.2 ETAPA DE OPERACIÓN (31,5 meses)**

En esta etapa EL CONTRATISTA debe iniciar y garantizar la operación de todos los servicios contratados, adicionalmente debe iniciar 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 (2 mes).** En este período se hará medición y seguimiento de ANS, sin embargo no se presentarán penalizaciones por este concepto.
  - **Finalización implementación de los servicios (1 mes):** En este periodo opera y finaliza instalaciones de alta complejidad.
  - **Estabilización de los Servicios (1 mes):** Ajustes a los procesos y procedimientos del modelo de gestión.
  - Implementación del SOC 4 meses a partir del inicio de la etapa de transición.
- **Operación de los servicios, medición y penalización de ANS para cada uno de los servicios, seguimiento línea base (29,5 meses).**

En esta etapa el contratista debe entregar como mínimo los informes que se relacionan en el Anexo 007 - REPORTES OPERACIÓN.

#### 6.4.3 ETAPA DE TRANSICIÓN SALIDA (2 meses)

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 al Contratista de la penalización de los servicios por el no cumplimiento de ANS y del desarrollo normal de la operación descrito en la ETAPA DE OPERACIÓN.

### 6.5 SERVICIOS

A continuación se realiza una breve descripción del estado de los servicios con que cuenta actualmente el ICBF.

#### 6.5.1 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 (Administrado por la empresa IFX Networks Colombia S.A.S, (se adquirió a través del acuerdo marco de precio y dicho servicio cuenta con unas condiciones, actualmente es operado con un plazo de 10 meses

hasta noviembre de 2015 y el ICBF esta adelantando las gestiones a fin de prorrogarlos hasta abril del 2017, después de esta fecha el ICBF tendrá que hacer una nueva cotización para adquirir el servicio para las vigencias 2017 y 2018)) en modalidad de HOUSING, en este Data Center Externo se encuentran cuatro (4) rack en donde se disponen los equipos que requieren alta disponibilidad, las aplicaciones y bases de datos, servidores de desarrollo, pruebas y producción. Adicionalmente el ICBF cuenta con un (1) 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.

De igual manera la Sede de la Dirección General cuenta con trece (13) centros de cableado distribuidos en forma equidistante en sus instalaciones; doce (12) de estos centros de cableados se encuentran aislados y cuentan con cerramiento y uno (1) se encuentran dentro de una oficina y no cuenta con encerramiento.

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 de 30 kva exclusiva para el centro de cómputo, piso falso, detectores de humedad, puerta de salida con barra anti pánico, pintura intumescente. Los anteriores sistemas no cuentan con garantía y fueron adquiridos en los siguientes años:

- UPS (enero de 2012)
- Aires Acondicionados (enero de 2012)
- Tableros Eléctricos regulados (enero de 2012)
- Sistema de extinción de incendios (enero de 2008)
- Transformador de aislamiento (enero de 2008)
- Tableros No regulados (enero de 2008)

Durante los últimos cinco años se han venido realizando mantenimientos preventivo de los equipos con la periodicidad que a continuación se indica:

- UPS (trimestral, 4 mantenimientos por año, último mantenimiento segundo trimestre de 2015)
- Aires Acondicionados (trimestral, 4 mantenimientos por año)
- Sistema de extinción de incendios (semestral, 2 mantenimientos por año)
- Transformador de aislamiento (semestral, 2 mantenimientos por año)
- Transformador de aislamiento (semestral, 2 verificaciones de cargas por año, se realizan en fechas diferentes a las programadas para los mantenimientos)
- Limpieza de Impurezas (semestral, 2 jornadas de limpieza por año)
- Tableros Eléctricos regulados y no regulados (bimensual, 1 verificación cada dos meses)

## **6.5.2 SERVIDORES**

El ICBF cuenta con 268 servidores de los cuales 76 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 172 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 y 20 servidores en cloud, las características de recursos de estos servidores en cloud se encuentran en el Anexo 012 - SERVIDORES EN CLOUD .

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 Windows centralizada en la cual se administra los servicios de toda la plataforma de Directorio Activo (DA), Dynamic Host Configuration Protocol (DHCP) y Domain Name System (DNS).

En la actualidad ICBF se encuentra en proceso de adquisición de:

- Infraestructura de convergencia para las sedes regionales la cual contará con soporte y garantía por 3 años.
- Infraestructura de Hyperconvergencia para el data center principal, esta infraestructura contará con soporte y garantía por 5 años.
- Renovación de la garantía y soporte por un periodo de 3 años de los dos (2) Enclosure c7000 y los 14 servidores blade de generación 6 y superior.

## **6.5.3 SEGURIDAD PERIMETRAL**

El ICBF actualmente cuenta con cuatro Appliances provistos por el actual proveedor durante la vigencia del contrato, 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 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) se realizan funcionalidades de gran granularidad en la configuración de la navegación, antispam, IPS, entre otros, adicionando las siguientes características:

- Antivirus
- Detección de Intrusos IDS
- Prevención de Intrusos IPS
- Application Control
- VPN Pptp, Ipsec, SSL
- Actualización automática de firmas
- Filtrado de Navegación

El proveedor actual de Infraestructura implemento dos clusters de seguridad perimetral (4 equipos en total) ubicados en el Data Center Externo y otros ubicados en el Centro de Computo de la SEDE DE LA DIRECCIÓN GENERAL.

El creciente uso de internet ha impulsado al ICBF a permitir a sus proveedores, funcionarios y otras entidades gubernamentales a 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 cifrado 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 cantidad de VPN son : Site to Site 6, SSL 774 y IpSec 82.

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. Recientemente se adquirió la solución McAfee de Antivirus con 11.000 licencias que funciona bajo arquitectura cliente – servidor gestionado por la consola EPO, 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).

#### **6.5.4 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.

#### **6.5.5 RESPALDOS (BACKUP)**

El ICBF genera los backup en cinta y en disco en servidores de su propiedad, se tienen configuradas dos aplicaciones del fabricante EMC, las cuales son Networker (Versión 7.6.5.5) en la cual se realizan respaldos a cinta a través de una librería StorageTek SL150 de 90 Slots con cuatro drives, dos tipo LTO5 y dos tipo LTO6 propiedad del actual proveedor la cual se retirará al finalizar el contrato de este operador, la cual deberá ser aporvisionada por el proveedor entrante.

La otra plataforma es Avamar propiedad del ICBF (Versión 6.1.2-47) caracterizada por la combinación de hardware y software que respalda 3 TB de información en disco y cuenta con deduplicación lo cual optimiza el uso de espacio al respaldar los datos iguales una única vez.

Adicionalmente el ICBF adelanta el proceso de actualización del licenciamiento de la solución de Networker, la compra de una solución de respaldo en disco de EMC y la adquisición de una librería.

En la actualidad el ICBF tiene un promedio de 200 políticas de Backup (en el Anexo 10 Backup se detallan las políticas) , más las solicitudes de backup por demanda divididas de la siguiente forma

| <b>Backup</b> | <b>Cantidad de Políticas</b> |
|---------------|------------------------------|
| Diarios       | 72                           |
| Semanales     | 34                           |
| Mensuales     | 69                           |
| Anuales       | 25                           |

Aproximadamente el número total de Backups lanzados mensualmente son de 1.200 con un tamaño promedio de 125 TB y se realizan 60 restauraciones.

La plataforma Avamar respalda 121 GB al mes, divididos en 31 políticas, 15 diarias, 6 semanales, 7 mensuales y 3 anuales la cual deberá ser administrada por El Contratista.

En el Anexo 007 - REPORTES OPERACIÓN se encuentra el inventario de políticas de backup, medios.

## 6.5.6 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 híbrida, ya que el 100% de los usuarios no se encuentran operando en la nube (10.000 usuarios en Office 365 y 3.500 On Premise), 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.

### 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 la cual está expuesta en el ANEXO 001-LINEA BASE-INFRAESTRUCTURA. A continuación se amplía la información sobre los servicios de Office 365 con que cuenta actualmente el ICBF:

**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). 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.

**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 2010 completamente licenciada, con una infraestructura de servicio híbrida, 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.

Este servicio está alojado de manera local en una infraestructura de 4 servidores virtuales en alta disponibilidad, 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.

- **Exchange Server On-premise:** Este servicio está alojado de manera local en una infraestructura de 4 servidores, funciona bajo sistemas operativos Microsoft Windows Server y Microsoft Exchange Server 2010. Este servicio permite la gestión de correo electrónico en conjunto con Exchange Online, 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.
- **Exchange Online:** Es el servicio que gestiona todo el correo electrónico en Office 365 (nube), el cual está configurado de forma híbrida 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.

**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 está soportada en Microsoft Lync Online y Microsoft Lync Server 2013, completamente licenciada. La infraestructura del servicio es híbrida, es decir On-premise-Nube, apoyada en servidores, conectada a la solución de video conferencia del ICBF a través de equipos Polycom.

- **Lync Server 2013 On-Premise:** 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 7X24X365 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.
- **Lync Online:** Este servicio permite la conexión a LYNC de todos los usuarios que tienen licencia de Office 365 (Nube) activa. Está configurado de forma híbrida 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.

**Sharepoint:** Permite tener sitios y subsitios para todas las áreas del ICBF con el fin de tener espacios de colaboración On-Line 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.

En este servicio se ubican actualmente 7 Sitios, pero se tiene proyectada la implementación en todas las Direcciones y Subdirecciones de SEDE DE LA DIRECCIÓN GENERAL 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 (Creación y administración de sitios actuales y nuevos, gestión de permisos y accesos, actualización de información por demanda, creación de sitios por demanda y gestión de requerimientos e incidentes) esta implementación que es totalmente lógica ya que este es un producto que se tiene por servicio y por demanda.

**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. 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.

## 6.5.7 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).

A continuación 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 y en el anexo Anexo 013 - INVENTARIO DE APLICACIONES se presenta una descripción de cada aplicación:

| Lenguaje programación | Nº de Aplicaciones |
|-----------------------|--------------------|
| .NET                  | 13                 |

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

### 6.5.8 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-LINEA BASE-INFRAESTRUCTURA se relacionan la cantidad de bases de datos con las que cuenta el ICBF, en la siguiente tabla se relacionan las bases de datos según el motor de base de datos.

| Motor Base de datos | Cantidad de base de datos |
|---------------------|---------------------------|
| SQL Server          | 91                        |
| MySQL               | 6                         |

### 6.5.9 GESTIÓN 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.
- Networker y Avamar para gestión de Backups.
- Microsoft System Center: La solución está completamente licenciada para los siguientes módulos:
  - Configuration Manager + Endpoint Protection
  - Service Manager (Módulo no esta implementado y no se implementará en este contrato)
  - Operation Manager (Módulo Implementado)
  - Virtual Machine Manager (Módulo Implementado)
  - Data Protection Manager (Módulo Implementado)
  - Orchestrator (Módulo Implementado)

De los cuales se encuentran en operación actualmente, Configuration Manager + Enpoint Protection, Virtual Machine Manager, WSUS para la administración de actualizaciones, KMS para la administración de licenciamiento (Relacionado con capítulo de servidores).

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.

### 6.5.10 REDES DE AREA LOCAL (LAN)

EL ICBF requiere el servicio de administración, operación, monitoreo los equipos activos de la red LAN garantizando la conexión de estaciones de trabajo, impresoras, teléfonos IP, cámaras

de videoconferencia, servidores, enrutadores y otros dispositivos habilitados para funcionar mediante protocolo IP (Internet Protocol) en las sedes de la Dirección General y Sedes Anexas, las cuales se describen en el Anexo 008 - EQUIPOS - RED LAN -WLAN. El ICBF está adelantando el proceso de adquisición de dispositivos de red (switches de acceso y switch core), algunos de los cuales se van a instalar en las sedes de la Dirección General y Sedes Anexas.

#### **6.5.11 RED INALAMBRICA (WLAN)**

Actualmente el servicio de RED INALAMBRICA (WLAN) permite a los funcionarios del ICBF equipados con dispositivos como desktops, laptops, Tablets y dispositivos inteligentes y similares conectarse a la red inalámbrica (WLAN), brindando movilidad y ampliando la cobertura de la red cableada dentro de las instalaciones físicas de la sede de la Dirección General y Sede de la Dirección de Información y Tecnología (Calle 57).

EL ICBF cuenta con 33 Accesspoint marca Aerohive AP-230, estos equipos poseen administración centralizada a través de un controlador con interfaz web en el portal del fabricante. Además cuenta en la sede de Dirección de Información y Tecnología con 7 access point marca HP MS-430, estos equipos no tienen administración centralizada y un access point marca Aerohive AP-230.

En la vigencia 2015 el ICBF está adelantando la adquisición de dispositivos de red inalámbrica, algunos de los cuales deberán ser instalados en la sede de la Dirección General y sedes Anexas.

#### **6.5.12 INTERNET MOVIL**

El ICBF cuenta con el servicio de Internet móvil mediante 320 módems USB tecnología 3.5G / 4G LTE y 3 Modems MiFi tecnología 3G/4G LTE con Navegación Ilimitada para los funcionarios del ICBF con el objeto de que puedan acceder a los contenidos y soluciones de Internet, Intranet, correo electrónico, aplicativos y demás servicios de red desde cualquier lugar en el territorio nacional. Los dispositivos modem son de propiedad del actual proveedor.

### **6.6 SERVICIOS REQUERIDOS**

En este capítulo se determinan el alcance y las especificaciones de los servicios a contratar, los cuales se describen a continuación:

### 6.6.1 CENTRO DE CÓMPUTO

El alcance de este servicio es administrar el Centro de Cómputo de la Sede de la Dirección General, con el fin de alojar el hardware y soportar los aplicativos y bases de datos de producción, desarrollo y pruebas. El servicio de administración incluye la operación de la infraestructura del Centro de Cómputo de la Sede de Dirección General, debe contar con soporte, monitoreo y gestión en modalidad 7X24X365.

EL ICBF requiere que en la administración del Centro de Cómputo de la Sede de la Dirección General se apliquen las mejores prácticas para la gerencia de proyectos, aseguramiento de la calidad, seguridad y gestión de servicios de tecnología de información.

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

La temperatura adecuada que se debe mantener para los dispositivos informáticos deberá oscilar entre 18° y 25° C (64,5° y 77° F), con una humedad relativa de entre 40 y 55%. Se requiere monitorear las condiciones ambientales del Centro de Cómputo, así como toda la infraestructura alojada en éste.

Las actividades mínimas requeridas en la administración del centro de cómputo de la Sede de la Dirección General son:

- Mantener el Centro de Cómputo de la SEDE DE LA DIRECCIÓN GENERAL, organizado y libre de obstrucciones.
- 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, Dispositivo de protección contra sobretensiones (DPS), fusibles u otros elementos de los tableros eléctricos o acometidas del centro de cómputo cuando se requiera.
- 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 del centro de cómputo.
- 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 connection) 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). La periodicidad mínima para estos mantenimientos es:
  - UPS (trimestral, 4 mantenimientos por año)
  - Aires Acondicionados (trimestral, 4 mantenimientos por año)
  - Sistema de extinción de incendios (semestral, 2 mantenimientos por año)
  - Transformador de aislamiento (semestral, 2 mantenimientos por año)
  - Transformador de aislamiento (semestral, 2 verificaciones de cargas por año, se realizan en fechas diferentes a las programadas para los mantenimientos)
  - Limpieza de Impurezas (semestral, 2 jornadas de limpieza por año)
  - Tableros Eléctricos regulados y no regulados (bimensual, 1 verificación cada dos meses)

Las anteriores actividades de administración se deben ejecutar periódicamente en forma proactiva, esto con el ánimo de anticiparse a posibles daños o fallas que puedan presentarse. En caso de presentarse un incidente que requiera el cambio de alguna parte, este debe realizarse dentro de los tiempos estipulados por la entidad.

- 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 equipos que se encuentran dentro del centro 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.
- Implementación de bitácora electrónica de registros del centro de cómputo de la sede de Dirección General.
- Mantener informado al Supervisor del contrato del ICBF o quien este delegue sobre el funcionamiento del Centro de Cómputo de la SEDE DE LA DIRECCIÓN GENERAL.
- 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.
- El ICBF requiere en cuanto a seguridad física, que:  
El Contratista implemente como mínimo controles físicos de registro de ingreso de personal autorizado tales: Control de acceso biométrico, bitácora electrónica de registros, 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.

- Cumplir los procedimientos y normas de seguridad descritas para Centros de Cómputo. (Norma TIA-942)

## 6.6.2 SERVIDORES

EL ICBF requiere la administración, gestión, operación, monitoreo, control y mantenimiento de la plataforma de servidores físicos, virtuales y en cloud, en arquitecturas de alta disponibilidad y redundancia, en infraestructura tradicional, convergente e hyperconvergente, 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. La plataforma de servidores debe estar disponible, administrada, monitoreada y en operación 7X24X365 y en concordancia con el ANEXO 001-LINEA BASE-INFRAESTRUCTURA. De igual forma se requiere la administración, monitoreo, ejecución de actualizaciones y garantizar la adecuada operación de los servicios de Directorio Activo, Dynamic Host Configuration Protocol (DHCP) y Domain Name Service (DNS).

El servicio además incluye:

- Presentar un plan de mejora continua donde el Contratista analice, diseñe, coordine y optimice las operaciones relacionadas con el sistema operativo e hypervisor; esto incluye las mejores prácticas del fabricante, actualizaciones, renombramiento de servidores, redistribución de clúster.
- La ejecución del plan de mejora continúa de las operaciones relacionadas con el sistema operativo e hypervisor, una vez analizados y aprobados por el ICBF y el Comité de Cambios del ICBF.
- La administración de parámetros de los sistemas operativos de acuerdo con las mejores prácticas del fabricante y lineamientos dados por el ICBF.
- Generar toda la documentación relacionada con bitácoras, fichas técnicas, seguimientos de control, manuales de procedimientos y hojas de vida de los equipos servidores y las máquinas virtuales.
- 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.
- La realización de 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.

- El servicio de migración de los sistemas de información del ICBF a servidores en Nube y continuar con la administración en la nueva infraestructura tecnológica de propiedad o contratada por el ICBF.
- La administración y monitoreo del 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.
- La administración y gestión del directorio activo a nivel de usuarios, grupos, unidades organizativas, políticas y directivas de seguridad, objetos de políticas de grupo, replicación de las bases de datos y demás operaciones que mantienen la correcta operatividad del mismo.
- El escalamiento de mantenimiento correctivo de equipos en garantía y diagnóstico de condiciones e infraestructura.
- El mantenimiento preventivo de equipos servidores y diagnóstico de condiciones e infraestructura.
- El análisis, diseño, propuesta y ejecución de las configuraciones y arreglos de servidores necesarios para garantizar la alta disponibilidad de la plataforma central de servicios básicos de red (Directorio Activo, DNS, DHCP); de tal forma que se garantice la disponibilidad 7X24X365 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.  
La realización por parte del Contratista de 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.
- Para los 20 servidores en Cloud que el ICBF adquirió a través del acuerdo marco de precio de centro de datos/nube privada, será responsabilidad del contratista:
  - Administración de sistema operativo
  - Administración de las bases de datos instaladas
  - Administración de las aplicaciones instaladas
  - Administración de los demás componentes y elementos que se encuentren instalados

### 6.6.3 SEGURIDAD INFORMATICA

#### 6.6.3.1 SEGURIDAD PERIMETRAL

EL ICBF para este servicio requiere el servicio de seguridad informática y perimetral que contenga instalación, configuración, administración, monitoreo y gestión de los firewalls de nueva generación, necesarios para la seguridad perimetral, de base de datos y aplicaciones del ICBF. La solución a proveer para administrar el servicio 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 y convergen en el Data Center Externo.

Para este componente se requiere suministrar, instalar, configurar, mantener, monitorear, gestionar los firewall de nueva generación, necesarios para la seguridad perimetral del ICBF.

Se 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 estar 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.
- El servicio deberá estar soportado por una plataforma que soporte la configuración en clúster mínimo hasta de ocho (8) miembros.
- Se deberá proveer 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.
- Este servicio deberá contar con las siguientes características de seguridad:

- Firewall
- IPS/IDS (Sistema de Prevención/Detección de Intrusos)
- Control de Aplicaciones
- Soportar Remote Access HTML 5, PPTP, L2TP sobre IPsec, IPSEC, Cliente VPN
- Protección contra Malware Avanzado
- AntiSpam
- Filtrado Web
- Data Leak Prevention en el motor antispam.
- 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 Gpbs
- Control de aplicaciones mínimo: 7.500 Usuarios de red
- Rendimiento de Protección contra Malware de 16 Gpbs
- Rendimiento AntiSpam: Mínimo 4000 Cuentas de Correo
- Rendimiento Filtrado Web: Mínimo 7500 Usuarios de red
- Debe contar con ocho (8) puertos GE de cobre
- Seis (6) Puertos 10 GE SFP+ con los transceivers.
- Conexiones TCP concurrentes: 20 Gbps
- Rendimiento VPN IPsec: 2.600 totalmente funcionales.
- Rendimiento VPN's SSL: (400) VPN's SSL totalmente funcionales.

- Rendimiento Mínimo de las Plataformas que soportan el Servicio Seguridad Sede Dirección Nacional del ICBF:

- Rendimiento mínimo de Firewall : 25 Gpbs
- Rendimiento de IPS/IDS: 7 Gpbs
- Debe contar con ocho (8) puertos GE de cobre
- Cuatro (4) Puertos 10 GE SFP+ con los transceivers.
- Control de aplicaciones mínimo: 2.000 Usuarios de red
- Filtrado Web: 2.000 Usuarios de red
- Rendimiento de Protección contra Malware de 10 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 tráfico 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.

- **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, con actualizaciones manuales de firmas y de patrones si el firewall no tiene acceso al internet.

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.

Debe ofrecerse la posibilidad de guardar los logs de los ataques identificados.

Actualización automática de firmas para el detector de intrusos durante la duración del contrato

- **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 mínimo de 1200 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, HTTPS, SMTP, 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, sin necesidad de requerir un 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, HTTPS, SMTP, 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.

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 incluida 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 incluida 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

La solución debe contar con funcionalidades de graylisting, BATV, inspección SPF, TLS, DKIM, La solución debe contar con funcionalidades para prevenir la pérdida o

fuga de información a través de los correos Data leakage (DLP), a través de listas de filtrado de contenido o expresiones regulares.

La solución debe permitir el cifrado de los correos electrónicos.

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 Filtrado 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 a través de la maquinas que utilizan 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, 14 y 16.

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 algún 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.

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, 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

- **Seguridad Perimetral (FW PERIMETRO Y FW INTERNO)**

La solución ofertada debe ser implementada con los appliances de Seguridad Perimetral que serán instalados en el Data Center Externo o utilizando firewalls virtuales. Los cuales deberán quedar totalmente implementados y con las políticas de seguridad requeridas por el ICBF, totalmente configuradas.

### 6.6.3.2 SEGURIDAD EN APLICACIONES WEB

En este componente se deberá 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 y la Intranet de la Entidad.

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

El servicio deberá contar con plataforma de Firewall de Aplicaciones Web, de propósito específico, estas plataformas solo deberán tener este rol de protección de aplicaciones.

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.

Este servicio deberá contar con las siguientes características de seguridad:

- Firewall de Aplicaciones Web especializado
- Protección Anti Defacement
- Protección DoS
- Auto Aprendizaje 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:

- **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 contrato.

- 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
- 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 anti defacement 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.

- **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. El alcance inicial será para 5 aplicaciones.

### 6.6.3.3 SEGURIDAD EN BASES DE DATOS

Para este componente se deberá instalar, configurar, mantener, monitorear, y gestionar los Agentes de Monitoreo 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.

Para el componente de seguridad en bases de datos debe cumplir con los siguientes requerimientos mínimos:

- 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
- Microsoft SQL Server 2014
- 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 mínimo de 90 bases de datos .
- El monitoreo de base de datos 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:

- **Modulo 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 Política
- 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 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 deben 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.

#### 6.6.3.4 ADMINISTRACIÓN DE ANTIVIRUS

Actualmente el ICBF cuenta con el Antivirus System Center Endpoint Protection 2012, en producción, que se utiliza en servidores y Clientes. Recientemente el ICBF adquirió la solución de antivirus McAfee que comprende:

| Descripción                                             | Cantidad | Periodo De Licencia      |
|---------------------------------------------------------|----------|--------------------------|
| CDBCDE-BA - MFE Complete Data Prtxn<br>P:1GL[P+]CompUpg | 600      | DEC/30/14 -<br>DEC/29/17 |
| FSWCKE-AA - MFE Vulnerability Mngr EN SW P:1 GL         | 11.000   | DEC/30/14 -<br>DEC/29/17 |
| CEECDE-AA - MFE Complete EP Protect Ent P:1 GL [P       | 11.000   | DEC/30/14 -<br>DEC/29/17 |

Las soluciones anteriores estarán bajo la administración del Contratista, para el caso del antivirus actual System Center Endpoint Protection una vez quede desactivado en una máquina no se requerirá más servicio de administración por parte del Contratista en dicha máquina y únicamente quedara administrando la nueva solución McAfee. Es posible que por licenciamiento se tenga que administrar los dos antivirus a nivel general. Las actualizaciones del antivirus llegan al servidor local ubicado en el Datacenter, y desde el mismo se despliegan las actualizaciones a los clientes teniendo especial cuidado de distribuir por grupos para no saturar los canales. La periodicidad de las mismas es por demanda, es decir depende de las actualizaciones que McAfee libere.

#### **6.6.3.5 SERVICIO SE CENTRO DE OPERACIÓN DE SEGURIDAD (SOC - Security Operation Center)**

El ICBF requiere el servicio de monitoreo SOC - Security Operation Center - para una gestión integrada de seguridad, operaciones y riesgos de TI en la plataforma tecnológica instalada en el ICBF.

El Contratista deberá presentar dentro de su propuesta la metodología que utilizará para dimensionar, instalar, implementar y hacer transferencia de conocimiento (funcional y técnica) el servicio de monitoreo objeto del presente documento, especificando etapas, recursos, entregables, herramientas, técnicas y metodologías a utilizar. Este servicio se debe implementar dentro de los primeros cuatro (4) meses desde el inicio del contrato.

- La solución requerida deberá incluir:
  - Gestión de Bitácoras y Correlación de Eventos de Seguridad en Tiempo Real (SIEM)
  - Gestión de Incidentes en Tiempo Real
  - Gestión de Configuraciones en Tiempo Real
- Condiciones obligatorias de las herramientas:
  - Las herramientas se deben integrar entre sí.

- Las herramientas deben ser de un mismo fabricante por facilidades en la integración.
- Especificaciones detalladas de las herramientas solicitadas para la implementación del SOC:
  - La solución deberá ser nueva en su totalidad y con las últimas versiones de software liberadas por el fabricante
  - No se aceptarán dentro de la oferta soluciones basadas en software libre.
  - La solución deberá ser con pares redundantes o unidades de respaldo y con mecanismos internos que ofrezcan alta disponibilidad.
  - La solución deberá tener una arquitectura modular, es decir con componentes dedicados para la colección, gestión y correlación de eventos.
  - La solución deberá soportar la cantidad de Eventos Por Segundo (EPS) sostenidos generados por 500 dispositivos/servidores de las cuales se obtendrán eventos.
  - La solución deberá contemplar la instalación y puesta a punto por personal certificado por parte del fabricante.
- Especificaciones técnicas Gestión de Bitácoras y Correlación de Eventos de Seguridad en Tiempo Real (SIEM)
  - Correlación de Eventos de Seguridad en tiempo real
    - La solución de correlación deberá utilizar infraestructura dedicada en appliance o servidor que centralice los componentes del motor de correlación. Los componentes que colectan los eventos deberán estar separados del motor de correlación.
    - La solución deberá permitir el diseño una arquitectura flexible y escalable, en la cual sea posible adicionar incrementos de capacidad de procesamiento de eventos por segundo sobre el licenciamiento base.
    - La solución deberá ofrecer como mínimo una capacidad de retención de 30 días de eventos en los componentes de correlación, en caso de ser necesaria ampliar la capacidad de retención, se podrá utilizar la solución de Almacenamiento y administración de registros de eventos del mismo fabricante.
    - La solución deberá incluir componentes dedicados a la recolección, normalización y categorización de eventos de seguridad. Estos componentes deberán ser concentrados en servidores de propósito específico de la misma marca del fabricante.

- La solución deberá proporcionar la capacidad de correlación basada en reglas (rule-based) y sin reglas (rule-less) ambas operando de manera concurrente.
- La solución de correlación deberá ser capaz de realizar la correlación en tiempo real y en memoria (sobre el flujo entrante de eventos), así como correlación histórica para eventos que han sido colectados fuera de línea (batch). Ambos mecanismos deberán operar de manera concurrente, esto es correlación en tiempo real y correlación histórica.
- Deberá realizar correlación geo-espacial, es decir, utilizando las direcciones IP de Internet del evento o información de la ubicación del dispositivo para la configuración de reglas para alertas de eventos relacionados y que ocurran en distintas zonas. Ej. El Usuario X realizando intentos de login en dos (2) localidades distintas de forma concurrente.
- Deberá permitir y definir ubicaciones físicas o lógicas internas, a las cuales se les podrán asignar coordenadas (latitud, longitud) que permitan identificar la ubicación geo-espacial de origen y destino de los eventos aún y cuando se encuentren bajo segmentos privados de direcciones IP.
- Deberá realizar correlación en tres (3) Dimensiones teniendo la habilidad de unificar y correlacionar eventos, información proveniente de herramientas de análisis de vulnerabilidades y criticidad de los activos o dispositivos que permita eliminar falsos positivos y evaluar de forma dinámica el nivel de riesgo considerando los factores mencionados.
- La solución de correlación deberá tener la capacidad de abstraer datos a partir de los eventos base provenientes de los dispositivos, tales como realizar el cálculo de algún valor (ej.: sumar o restar, redondear) o derivar algún dato particular (ej: día del mes, hora del día) que permita realizar un análisis de eventos basándose en el contexto (ej. Generar una alerta si el evento se reporta en un horario no productivo a partir de la hora del día).
- El motor de correlación deberá estar basado en firmas de seguridad así como en la detección de comportamiento anómalo mediante correlación estadística a través de cálculos de promedio, desviación estándar, curtosis, varianza.
- La solución de correlación de eventos deberá permitir probar reglas de correlación sobre eventos históricos con una ventana de tiempo configurable, que permitan afinar puntualmente las reglas de correlación previo a su despliegue en ambientes productivos.

- La solución de correlación deberá permitir integrar en el proceso de análisis en tiempo real eventos de correlación, es decir, adicional a los eventos base recibidos por los colectores de eventos, analizar los eventos de correlación previamente identificados, a fin de identificar amenazas o patrones más complejos.
- La solución de correlación deberá contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores:
  - Importancia del evento
  - Criticidad del activo
  - Vulnerabilidades asociadas
  - Antecedentes previos sobre el origen, destino o ambos.
- La solución de correlación de eventos deberá incorporar mecanismos internos de protección, tales como deshabilitar reglas que incurran en recursividad, o deshabilitar temporalmente reglas que generen un número elevado de alertas.
- La solución de correlación deberá incluir herramientas para el monitoreo gráfico sobre el uso y activación de las reglas de correlación.
- La solución de correlación deberá utilizar un motor de almacenamiento propietario optimizado para la correlación, retención y búsqueda sobre altas tasas de eventos.
- La solución de correlación deberá contar con un único repositorio para el almacenamiento de todos los eventos enviados y normalizados desde su origen por los conectores, éste repositorio deberá guardar en su totalidad los distintos elementos de cada evento en campos específicos independiente del tipo de dispositivo o aplicativo que la genere, permitiendo así la definición de contenido de correlación entre distintos tipos de dispositivos (firewalls, IDPs, Sistemas Operativos, conocido como cross device correlation) sin la necesidad de utilizar estructuras complejas o lenguajes de acceso a datos para la consulta y unión de dato.
- La solución deberá ofrecer la capacidad de archivar eventos a un almacenamiento fuera de línea, complementando y aumentando la capacidad total de retención, estos archivos de eventos podrán ser reactivados bajo demanda para poder realizar búsquedas y correlación histórica de eventos.

- La Solución de Correlación de Eventos deberá proporcionar un modulo integrado para la gestión de casos (tickets) de seguridad permitiendo asociar eventos a acciones tales como enviar una notificación al equipo de operadores, abrir y asignar un caso a un usuario para su investigación o ejecutar un script a partir de la identificación de un incidente de seguridad.
- La solución debe contar con un flujo de trabajo (workflow) nativo, automatizado y con el manejo de niveles de escalamiento parametrizable para el manejo de incidentes de seguridad, así como permitir la integración de soluciones de mesa de ayuda de terceros.
- La Solución de Correlación de Eventos deberá contar con tableros gráficos (dashboards) para el monitoreo de datos y eventos en tiempo real. Un tablero gráfico o dashboard deberá contener y agrupar una o más representaciones gráficas o tabulares de los datos bajo una misma vista.
- La Solución de Correlación de Eventos deberá permitir desplegar más de un tableros gráficos (dashboards) de forma concurrente y bajo una misma sesión de usuario abierta y su actualización deberá ser en tiempo real sin la intervención del usuario o refresco manual.
- Los tableros gráficos (dashboards) de eventos deberán ser personalizables por los usuarios de la Solución de Correlación de Eventos.
- La solución deberá proporcionar una interface de administración gráfica (GUI) con licenciamiento para 3 usuarios nombrados de consola para el personal operativo y administrativo de la solución, así como una interface de solo lectura para un mínimo de 25 usuarios tipo web, diseñada para el personal de monitoreo y personal no técnico. Ésta última consola debe ser únicamente accesible vía web.
- La Interfaz de administración gráfica de la solución de correlación deberá desplegar los eventos recolectados de forma estructurada, es decir deberán ser previamente analizados y normalizados en su totalidad y distribuidos en los campos específicos con el fin de permitir y facilitar el análisis de eventos incluso de múltiples tipos de dispositivos.
- La interfaz de administración gráfica de la solución de correlación deberá permitir la importación de gráficos a manera de diagramas que permitan asociar tableros gráficos visuales (dashboards) a una determinada porción o segmento del diagrama para proveer de una visualización lógica y estado situacional de la seguridad en determinada zona de la red o negocio.

- La interfaz de administración gráfica de la solución de correlación de eventos deberá tener la capacidad de graficar la ruta y comportamiento de un conjunto de eventos a través del uso de nodos, de tal forma que sea posible generar una abstracción visual de los mismos que incluya como mínimo las siguientes vistas:
  - Jerárquica
  - Orgánica
  - Circular
- La Interfaz de administración gráfica de la solución de correlación deberá ofrecer herramientas integradas que permitan analizar la información proveniente de tableros gráficos (dashboards) con la capacidad de profundizar para identificar la causa raíz (drill-down) sin la ejecución de componentes o aplicaciones externas.
- La interfaz de administración gráfica de la solución de correlación deberá desplegar los eventos de correlación, así como el evento o eventos base relacionados, pudiendo ver la cadena de eventos bajo la misma vista.
- La interfaz de administración gráfica de la solución deberá permitir generar una base de conocimiento (KB) a través de las cuales se pueda generar y consultar información, protocolos a seguir y asociarlos a eventos, casos, reportes.
- La interfaz de administración gráfica deberá permitir agregar anotaciones en los casos (tickets).
- La Interfaz de administración gráfica de la solución de correlación de eventos deberá permitir la integración para la ejecución de aplicaciones o scripts externos, pudiendo incluso pasar parámetros o información, tales como herramientas para la captura de paquetes de red, herramientas de geo-localización, traza de rutas, búsquedas de dominios en whois.
- La interfaz de administración deberá tener la capacidad de crear comandos de integración que permita la interacción de la solución de correlación con herramientas o soluciones de terceros, tales como abrir un URL en un navegador, ejecutar una herramienta o script para efectuar la remediación automática de un incidente, efectuar una búsqueda en Whois o Google.
- La solución deberá soportar un mecanismo de autenticación nativo además de soportar mecanismos alternativos como: Microsoft Active Directory, Autenticación de doble factor, LDAP y componentes JAAS.

- La solución debe poder generar controles de acceso granulares basado en roles (RBAC) permitiendo la segregación de funciones y acceso a eventos, obedeciendo al principio de mínimo privilegio.
- La solución deberá ser capaz de enviar alertas vía email, mensajes SMS por protocolo SNPP, traps SNMPv1, SNMPv2 y SNMPv3 así como notificaciones directo a la consola de administración.
- La solución de correlación deberá tener la capacidad de crear flujos de trabajo o casos de forma automatizada e incluso de alimentar casos (tickets) ya existentes como mecanismos de acción de las reglas de correlación.
- La solución de correlación deberá soportar el apilamiento de eventos, es decir, no realizar acciones subsecuentes para eventos repetitivos, pudiendo controlar la forma en que se generan las acciones evitando el desbordamiento de notificaciones o alertas. Ejemplos de apilamiento:
  - Crear una notificación bajo el primer evento o umbral
  - Crear un caso en el primer evento/umbral y agregar a un caso existente en eventos subsecuentes.
  - Crear un caso o notificación en cada evento/umbral.
- La solución deberá ser compatible con el estándar libre para la administración y formato común de eventos ofreciendo más de 400 campos para la normalización y distribución de los distintos campos obtenidos a partir de los eventos recolectados.
- La Solución de Correlación debe permitir organizar y clasificar a los activos monitoreados bajo categorías independientes y personalizables, permitiendo y favoreciendo su utilización en filtros, monitores gráficos, reglas de correlación, entre otros para eliminación de falsos positivos. Ejemplos de categorías para la clasificación de activos:
  - Nivel de Criticidad
  - Función dentro de la organización
  - Aplicativo residente
  - Nivel de seguridad de la Información Almacenada
  - Nivel de Acceso
- La solución de correlación deberá soportar la definición de listas de observación estáticas y dinámicas (listas blancas, negras, sospechosos,

hostiles, de exclusión) que puedan ser actualizadas y consultadas de forma automática en el proceso de correlación en tiempo real, para identificar ataques o atacantes recurrentes, escalamiento de amenazas persistentes, entre otros.

- Las listas deberán soportar no menos de veinte (20) campos definidos por el usuario.
- La solución de correlación deberá soportar la definición de listas de sesión en adición a las listas de observación. Las listas de sesión tendrán la capacidad de mantener un registro detallado de inicio y cierre que puedan ser utilizadas en la correlación de eventos y dispositivos orientados a sesión como VPN, DHCP, Active Directory, etc.
- Debe incluir contenido en modo de filtros, reglas de correlación, monitores gráficos y reportes pre-configurados de monitoreo de dispositivos de red perimetral, enfocado a las mejores prácticas de seguridad y ataques más comunes.
- La solución de correlación deberá tener la capacidad de integrar un servicio de suscripción de inteligencia de seguridad generado por el mismo fabricante de la solución, a través del cual se pueda recopilar de manera automática y periódica un listado de los dominios y direcciones IP que presenten una actividad maliciosa en internet como exploits, amenazas combinadas, botnets, malware, phishing, spam. A través de esta información se deberá realizar la correlación automática de los eventos de seguridad.
- La solución deberá ser capaz de generar eventos y alertas cuando alguno de sus componentes falle.
- La solución deberá soportar los protocolos SSLv2, SSLv3 y TLSv1 para el envío cifrado de información entre todos sus componentes.
- La solución de correlación deberá permitir realizar correlación histórica, es decir de eventos que ya se encuentran almacenados en la base de datos o que incluso pueden ser reactivados. Este método de correlación deberá ser adicional a las capacidades de correlación en tiempo real realizadas por la herramienta.
- La solución de correlación de eventos deberá permitir modelar y configurar las distintas redes, con la capacidad de diferenciar redes con traslape (overlapping), zonas y recursos monitoreados, que puedan ser cargados a

partir de una lista de activos generada por plataformas de gestión de configuraciones (CMDB).

- La solución de correlación de eventos deberá permitir la correlación de flujos de componentes de conectividad NetFlow, J-Flow y s-flow sin integrar componentes o herramientas de terceros.
- La solución de correlación de eventos deberá contar con funcionalidades integradas en la interfaz de administración gráfica para la definición, ejecución, calendarización y entrega automatizada de reportes ejecutivos y detallados en los siguientes formatos:
  - PDF
  - CSV
  - HTML
  - RTF
- La solución de correlación de eventos deberá contar con un mecanismo que optimice la generación de reportes sobre periodos largos de tiempo para no hacer una consulta masiva en el repositorio de eventos que implique una degradación en el desempeño del componente de correlación.
- No se acepta la integración de productos o programas de terceros para la generación de reportes, tales como Crystal Reports y/o Jasper Reports o similares, aún y cuando esté incluido dentro de la licencia de la solución, ya que se requiere una interfaz única que centralice todos los componentes y recursos necesarios para el monitoreo, administración y reporte de los eventos, correlación e incidentes de seguridad.
- La solución debe proveer documentación en línea por medio de la GUI para ayudar a los usuarios a entender las funciones de cada pantalla.

○ Gestión de Bitacoras

- La solución deberá tener la capacidad de recibir logs en formato crudo (RAW) a través de los siguientes mecanismos:
  - Syslog (TCP o UDP).
  - Transferencia remota de archivos con logs crudos por SCP (Secure Copy), sftp (Secure FTP) o ftp.
  - Archivos de logs en sistemas de archivos remotos mediante NFS y/o CIFS

- En adición a la colección de datos en formato crudo, la solución debe tener la capacidad de recibir de manera simultánea eventos estructurados provenientes de los componentes dedicados a la recolección de eventos.
- La solución deberá permitir la estructuración de bitácoras crudas (raw) de fuentes comunes como Apache, BlueCoat, VMWare ESX, Cisco PIX dentro de la misma solución, es decir sin integrar los componentes de recolección de eventos
- La solución deberá tener una capacidad efectiva de almacenamiento en línea de eventos de 42 TB de bitácoras posterior a la aplicación de la compresión de eventos.
- La Solución de almacenamiento y administración de registros de eventos deberá integrarse de forma bidireccional con la solución de correlación del mismo fabricante.
- La solución deberá ser de tipo appliance de propósito específico, con sistema operativo Red Hat Enterprise Linux 5.5 o posterior a 64 bits.
- La solución deberá realizar indexación basada en campos, así como indexación completa de texto (full-text indexing).
- La solución deberá incluir una interface administrativa basada en Web para la configuración, monitoreo, análisis y explotación de eventos, así como una interface de administración vía CLI (línea de comandos).
- La interfaz basada en Web deberá ser compatible con navegadores Internet Explorer y Firefox/Mozilla.
- La solución deberá permitir desplegar en distintos paneles gráficos o dashboards los sumarios de distintos indicadores o métricas de seguridad, operaciones, etc., mismos que deberán ser actualizados de manera automática en intervalos de tiempo configurables.
- Los paneles gráficos deberán tener la capacidad de profundizar al detalle de los eventos (drill-down) dando clic en cualquier área gráfica.
- La solución deberá contar con una Interfaz para la programación de aplicaciones (API), que permitirá incorporar las funcionalidades de búsqueda y reporte de eventos en aplicaciones propietarias de la convocante.

- La solución deberá permitir generar de forma automatizada o sobre demanda un respaldo de la configuración de la unidad a un servidor remoto.
- La solución deberá permitir definir controles de acceso granulares para limitar los privilegios, así mismo deberá permitir restringir el acceso a eventos bajo la definición de filtros de búsquedas
- La solución deberá permitir definir grupos de usuarios, sobre los cuales se le aplicarán los controles de acceso y visualización de cierto tipo de eventos.
- La solución debe ser capaz de almacenar las bitácoras en crudo en adición a la bitácora normalizada.
- La solución deberá incorporar mecanismos de generación y verificación de la integridad de la información almacenada de acuerdo a la publicación especial NIST 800-92.
- La solución deberá contar con mecanismos basados en RAID 5 para la protección de la información, así como para ofrecer altos niveles de desempeño en la lectura y escritura de datos.
- La solución deberá ser capaz de recibir eventos multi-línea y manejarlo como un solo registro. Se entiende por multi-línea aquellos eventos que se extienden a más de una línea, por ejemplo, registros de excepciones o errores.
- La solución propuesta debe manejar una tasa de compresión de eventos en el orden de 10 a 1.
- La solución deberá ser capaz de realizar de forma concurrente la recepción de altos volúmenes de eventos, búsquedas rápidas de eventos y almacenamiento de dichos eventos, sin comprometer el desempeño de ninguno de estos tres parámetros.
- La solución deberá permitir la escalabilidad, mediante el apilamiento de múltiples soluciones de administración de eventos formando una comunidad, incrementando linealmente la capacidad de almacenamiento y la realizar búsquedas y reportes de forma distribuida entre la comunidad.
- La solución deberá permitir realizar búsquedas estructuradas o basadas en campos, es decir a partir de los eventos que han sido normalizados a un formato común por los componentes de colección.

- La solución deberá contar con un asistente para la definición de búsquedas estructuradas, sin que se tenga que introducir manualmente ningún criterio de búsqueda.
- Así mismo la solución deberá asistir en el momento de ingresar manualmente la cadena de búsqueda, reduciendo el tiempo requerido para generar búsquedas y explotar eventos, a través del despliegue de las siguientes ayudas:
  - Histórico de búsquedas.
  - Operadores recientemente utilizados
  - Ejemplos de utilización de operadores
  - Sugerencia de operadores de búsqueda
  - Listado de campos disponibles
  - Listado de operadores disponible
- La solución deberá permitir realizar búsquedas no estructuradas, es decir basadas en texto o palabras clave (keyword), ya sea sobre eventos normalizados o eventos crudos (Raw), así como definir expresiones regulares.
- La solución deberá contar con un asistente que genere de forma automática expresiones regulares sobre eventos crudos, con lo que se podrán analizar en detalle campos o atributos específicos provenientes de los eventos crudos.
- La solución deberá permitir combinar las búsquedas estructuradas y no estructuradas bajo una misma cadena de búsqueda (query). La solución deberá permitir integrar lógica booleana (AND, OR, NOT, etc) en los criterios de búsqueda para poder obtener resultados precisos.
- La solución deberá ser capaz de profundizar en los resultados previamente obtenidos de las búsquedas estructuradas y/o no estructuradas a través del uso de operadores de búsqueda, los cuales extraerán información de interés permitiendo obtener información como el top N de eventos, promedio (avg), ordenar (sort), últimos N eventos (last), esta funcionalidad es conocida como análisis bottom-up.
- Las búsquedas definidas dentro de la solución deberán poder ser guardadas para ser invocadas posteriormente.
- Las búsquedas guardadas podrán ser calendarizadas para que se ejecuten de forma automática y los resultados sean exportados.

- Los operadores de búsqueda deberán generar sumarios gráficos en modo de Barras, Columnas, Pie, Area, Línea, Columnas apiladas, Barras apiladas.
- Los operadores de búsqueda deberán permitir agrupar múltiples series de datos numéricos en un mismo gráfico. Ej. cuando se requieran comparar promedios contra sumatorias de un campo en particular.
- Los operadores de búsqueda deberán generar reportes al vuelo, con la posibilidad de exportar la información obtenida en modo CSV o PDF, sin la necesidad de ingresar en el módulo de reportes
- La solución deberá permitir buscar eventos en ventanas de tiempo predefinidas (últimos 30 minutos, últimas 2 horas, etc), o configurables (indicando inicio y fin de la búsqueda).
- La solución deberá permitir definir vistas en las cuales se organicen y visualicen únicamente los campos requeridos como resultados de las búsquedas.
- La solución deberá identificar automáticamente los dispositivos de los cuales recibe eventos, creando de forma automáticamente un objeto asociado a dicho dispositivo. Así mismo deberá permitir definir de forma manual dispositivos.
- La solución deberá permitir generar grupos de dispositivos asociando los dispositivos generados manual o automáticamente y asignarles un nombre para su identificación.
- La solución deberá permitir políticas de retención de eventos basadas en tamaño (GB) o tiempo (Días), las cuales aplicarán de forma independiente a cada grupo de almacenamiento de eventos, lo que permitirá contar con un almacenamiento de eventos inteligente y auto administrado.
- La solución deberá permitir ampliar o reducir en cualquier momento el tamaño del grupo de almacenamiento de eventos
- La solución deberá permitir definir reglas de almacenamiento de eventos, a través de la definición de relaciones entre grupos de dispositivos y grupos de almacenamiento. Las reglas de almacenamiento definirán en qué grupo de almacenamiento se guardarán los eventos provenientes de múltiples dispositivos.

- La solución deberá permitir focalizar las búsquedas ya sea a nivel de grupos de dispositivos y grupos de almacenamiento de eventos.
- La solución debe ofrecer la capacidad de exportar los resultados de las búsquedas ya sea a través de un punto de montaje NFS, CIFS, o bien un archivo descargable en la consola web, ya sea en formato PDF o CSV para procesamiento posterior.
- La solución deberá permitir reenviar ya sea de forma selectiva o en su totalidad los eventos que recibe hacia otros hosts, a través de protocolos TCP, UDP, Syslog, así como al correlacionador de eventos del mismo fabricante.
- La solución deberá ofrecer la funcionalidad de archivar todos los eventos existentes en su almacenamiento interno hacia un almacenamiento externo y fuera de línea (offline), utilizando los protocolos NFS o CIFS. Los archivos de eventos podrán ser posteriormente referenciados de manera remota para poder realizar búsquedas sobre la información que ya no se encuentre inmediatamente disponible o en línea.
- La solución deberá ofrecer la capacidad de archivar eventos en ubicaciones (CIFS o NFS) separadas e independientes para cada grupo de almacenamiento de eventos.
- La funcionalidad de archivado de eventos podrá ser ejecutada de forma manual o calendarizada
- El archivado y/o recarga de archivos de eventos podrá ser realizado de forma unitaria (por día) o masiva (múltiples días) bajo una sola operación.
- La solución deberá contar con un módulo integrado para la ejecución de reportes sobre los eventos.
- Los reportes generados podrán ser de tipo ejecutivos (gráficos), detallados (matriz/tabla) o una combinación de ambos.
- El módulo de reportes, deberá permitir generar un reporte, ya sea desde cero o bien copiando y modificando reportes existentes.
- La solución deberá ofrecer la capacidad de generar reportes calendarizados, con la opción de entrega por correo electrónico, publicación dentro de la misma solución, o almacenarlo localmente.

- Los reportes generados deberán ser exportables en los siguientes formatos:
  - HTML
  - PDF
  - Microsoft Excel
  - CSV
  - Microsoft Word
  - XML
- La solución deberá integrar reportes tipo drill-down, es decir, a partir de los resultados de un reporte, seleccionar algún resultado y automáticamente ser transferido a un nuevo reporte que proporcione un mayor nivel de detalle.
- El módulo de reportes, deberá permitir aceptar parámetros previo a la ejecución de un reporte, para poder focalizar los resultados del mismo. Ej.: Ingresar el nombre de usuario, nombre del dispositivo, etc.
- La solución debe contar con una base preinstalada que comprenda como mínimo 130 reportes, distribuidos en las siguientes categorías:
  - Top 5 SANS
  - Monitoreo de Red
  - Monitoreo de Intrusiones
  - Monitoreo de la configuración
  - Reportes Anti-virus
  - Reportes de múltiples dispositivos (cross-device)
  - Reportes de base de datos
  - Reportes de firewalls
  - Reportes de administración de identidades.
  - Reportes de IPS/IDS.
  - Reportes de red
  - Reportes de sistemas operativos
  - Reportes de VPN.
- Recolección de eventos de seguridad
  - La solución SIEM deberá ser integrable “fuera de la caja” (out-of-the-box) como mínimo con más de 300 dispositivos y aplicaciones de más de 100 fabricantes lo cual evitara tener personal dedicado a la modificación de los

formatos de logs, mediante componentes denominados conectores/colectores.

- Los componentes que realizan la recolección de eventos deberán ser provisionados en servidores o appliance de propósito específico para la solución SIEM, así mismo se requiere el provisionamiento de una unidad redundante que sirva como respaldo en caso de falla.
- Los componentes que realizan la recolección de eventos (conectores) deberán enviar los eventos hacia la solución SIEM a través del protocolo de transporte TCP y con técnicas de cifrado SSL (Secure Sockets Layer).
- Los colectores de eventos remotos o distribuidos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia la solución, salvo que se requiera habilitar bajo demanda el envío asíncrono de eventos.
- Los componentes que realizan la recolección de eventos (conectores) deberán enviar los eventos hacia la solución SIEM a través del protocolo de transporte TCP y con técnicas de cifrado SSL (Secure Sockets Layer). No se permite el uso de protocolo Syslog/Syslog-ng TCP ni UDP para el envío de eventos de conectores hacia el SIEM.
- Los colectores de eventos remotos o distribuidos deberán enviar en todo momento y en tiempo real los eventos recolectados hacia la solución, salvo que se requiera habilitar bajo demanda el envío asíncrono de eventos.
- Los colectores de eventos deberán enriquecer mediante categorías los eventos obtenidos en los componentes de recolección a fin de permitir la comprensión y el significado del evento, sin la necesidad de tener conocimiento previo de la bitácora, las categorías requeridas son:
  - Objeto referido en el evento (Aplicación, Usuario, etc).
  - Comportamiento sobre dicho evento (Acceso, Ejecución, Autenticación, etc).
  - Resultado de dicha acción (Intento, Éxito, Fallido).
  - Técnica utilizada
  - Importancia del evento
  - Grupo o familia del dispositivo (IDS, Sistema Operativo, etc.)
- La solución SIEM debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente “fuera de la caja” (tales como aplicaciones o desarrollos hechos en casa) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer,

obtener, normalizar y categorizar los eventos registrados en las siguientes fuentes:

- Archivos de logs (bitácoras) con campos delimitados
  - Archivos de logs (bitácoras) de longitud variable (no delimitados).
  - Bases de datos relacionales por conexión ODBC
  - Bases de datos relacionales por conexión JDBC
  - Traps de protocolo SNMP
  - Eventos enviados por protocolo Syslog
  - Archivos con formato XML
- 
- El conjunto de herramientas para recolectar eventos de fuentes no soportadas por la solución de correlación deberán permitir la creación y distribución de dichos componentes de forma gratuita, sin importar el número de conectores desplegados.
  - El conjunto de herramientas para definir la lógica para extraer, obtener, normalizar y categorizar los eventos a correlacionar por la solución no deberán utilizar ningún lenguaje de programación JavaScript ni XML para definir la lógica de recolección de eventos. Únicamente se permitirá el uso de expresiones regulares o REGEX para definir patrones de búsqueda de cadenas de texto.
  - La solución deberá soportar la colección de eventos en modo agent-less y que permita la colección de múltiples dispositivos desde un único componente de captura.
  - La colección de eventos de equipos Windows deberá ser realizada a través de Microsoft RPC de manera remota, es decir sin la instalación de agentes.
  - Los componentes que realizan la recolección de eventos deberán realizar desde el origen la normalización completa de los eventos, es decir únicamente enviarán a la solución los eventos previamente estructurados en campos específicos para la correlación, retención, análisis y reporte de los eventos.
  - Los componentes que realizan la recolección de eventos podrán bajo demanda preservar el campo en crudo en adición al evento previamente normalizado.
  - Los componentes que realizan la recolección de eventos deberán tener la capacidad de generar una firma o huella digital sobre los eventos crudos mediante el uso de algoritmos criptográficos de una sola vía, así mismo los

conectores deberán tener la capacidad de validar la integridad de estos eventos.

- Los componentes que realizan la recolección de eventos deberán utilizar el protocolo TCP como medio de transporte hacia la solución de correlación, verificando constantemente el estado de la conexión por medio de un pulso o “Heartbeat”. Ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache.
- Los componentes que realizan la recolección de eventos podrán agregar etiquetas en campos adicionales sobre los eventos con información proveniente de la configuración y modelado de la red definida en el motor de correlación tales como información de la red, ubicación geográfica, unidad de negocio, que favorezca y optimice el proceso de correlación de eventos.
- Los componentes que realizan la recolección de eventos deberán tener funciones para alcanzar un destino redundante así cuando el destino primario no esté disponible el dispositivo de recolección automáticamente iniciara el envío de los datos al destino secundario.
- Los componentes que realizan la recolección de eventos deberán tener la capacidad de enviar los datos a múltiples destinos primarios de forma simultánea.
- La transmisión de los datos entre los componentes recolectores de eventos y el motor de correlación deberán utilizar mecanismos de compresión de datos.
- La solución debe permitir configurar controles de uso de ancho de banda para el envío de los eventos recolectados, así como priorizar las transacciones críticas para su envío inmediato.
- La solución deber permitir configurar el retraso voluntario en el envío de eventos al motor de correlación basado en horarios, de tal forma que el colector de eventos guarde en su cache los eventos y envíe eventos con prioridad alta durante el horario configurado. Una vez finalizado el horario, se enviarán los eventos de más baja prioridad.

- La solución propuesta deberá tener la capacidad de agregación de eventos similares basada en campos definidos por el usuario y bajo una ventana de tiempo parametrizable, enviando al motor de correlación eventos de tipo agregación que contienen la cuenta de eventos previamente agregados en conformidad a la publicación NIST 800-92.
  - Los componentes que realizan la recolección de eventos deberán tener la capacidad de filtrado de eventos particulares desde el origen, con lo que se reducirá el volumen de eventos que recibirá el motor de correlación en conformidad a la publicación NIST 800-92.
  - Los componentes que realizan la recolección de eventos deberán ofrecer la capacidad de ajuste en la hora de los eventos, en el caso de que el dispositivo que genere el evento no cuente con la hora correcta o no tenga configurado un servidor de NTP.
  - Los componentes que realizan la recolección de eventos deberán ofrecer la capacidad de ofuscar campos sensibles por la sustitución de algoritmos criptográficos de una sola vía.
  - Los componentes que realizan la recolección de eventos tendrán la capacidad de administración y actualización remota, sin la necesidad de realizar cambios, ajustes o actualizaciones directamente en el componente.
  - Los componentes que realizan la recolección de eventos deberán contar con múltiples perfiles de configuración, los cuales entrarán en funcionamiento en función de horarios preestablecidos.
- Especificaciones técnicas de la Solución de Gestión de Incidentes en Tiempo Real

Los siguientes requerimientos deben ser configurados, parametrizados y operados por el contratista:

- Administración de operaciones de seguridad
  - La Administración de operaciones de seguridad para la solución de incidentes de seguridad debe seguir estándares de IT internacionales y en particular las mejores prácticas de ITIL V3.
  - Se requiere la visualización e integración con el catálogo de servicios de seguridad informática y servicios de TI.

- Se requiere disponer de un dashboard de seguridad informática y perimetral que presente información de las diferentes funcionalidades en forma integrada.
- Se requiere que la solución permita registrar de forma automática los eventos generados por las diferentes herramientas de monitoreo utilizadas para la operación del servicio de seguridad informática y perimetral del ICBF
- Se debe realizar la configuración de reglas de escalamiento.
- Se requiere configurar el autoservicio “self service” para usuarios finales del servicio de seguridad informática y perimetral.
- La solución de seguridad informática y perimetral debe soportar la configuración de niveles de servicio.
- La solución de seguridad informática y perimetral debe soportar el envío de alertas e información sobre incidentes, problemas y cambios ante la proximidad o incumplimiento de tiempos definidos.
- La solución de seguridad informática y perimetral debe tener la capacidad de enviar mails configurable a usuarios, operadores o grupos definidos en el sistema.
- Se requiere que hagan uso de la base de datos de conocimiento (Adicionar, modificar, consultar la KDB) de la herramienta de gestión del ICBF.
- Se requiere que gestione los incidentes, problemas, cambios y CI en la herramienta de gestión del ICBF.
- Se requiere que con el servicio de seguridad informática y perimetral y la herramienta de gestión del ICBF se generen estadísticas, mediciones de tiempos de atención, tiempos de espera y tiempos asociados a los casos registrados.
- Se requiere que la solución permita la consulta histórica de información de los casos.
- Administración de incidentes de seguridad
  - Se requiere que la solución de gestión de incidentes siga estándares de IT internacionales y en particular las mejores prácticas de ITIL V3
  - Se requiere registro, seguimiento y control de los incidentes.

- Mantener la información integrada de incidentes, en el mismo sistema que posee la información de problemas, errores y cambios.
- Clasificar los incidentes de acuerdo a criterio de prioridad, severidad, impacto y urgencia.
- Permitir la configuración de reglas de escalamiento.
- Alertar a una segunda línea de soporte (especialistas), en caso que sea necesario.
- Debe disponer de información de errores conocidos.
- Debe registrar todas las actividades en relación al incidente.
- Se requiere que la solución reciba de forma automática los eventos de herramientas de gestión de infraestructura y que permita crear automáticamente un incidente.
- Permitir a los operadores involucrados en la Administración de operaciones de seguridad, visualizar los incidentes previos de la persona que se está comunicando.
- Debe informar a la persona que registra el caso el tiempo estimado de resolución de acuerdo al objetivo establecido por la categoría, el tipo de usuario, el CI asociado o la ubicación del usuario.
- Notificar automáticamente del cierre de un incidente a todos los involucrados con el mismo, en particular al usuario.
- Debe entregar reportes solicitados por el ICBF resultado de la operación y gestión del servicio de seguridad informática y perimetral.
- Administración de Niveles de Servicio
  - Gestionar los Niveles de Servicio con estándares de IT internacionales y en particular las mejores prácticas de ITIL V3
  - Se requiere que los niveles de servicio (ANS) soportados por la solución, deben ser definibles y susceptibles de rastreo en cualquier momento del tiempo.
  - Llevar el control para la actualizaciones de los niveles de servicio (programación). Es decir, monitorear, controlar y administrar las vigencias de los acuerdos de Niveles de Servicio.

- Se debe realizar seguimientos, análisis de tendencias, estadísticas, reportes de no cumplimientos del ANS y SLO
- Revisar en forma historica los cumplimientos de los ANS.
- Se requiere informes en donde se incorporen los detalles del funcionamiento del Acuerdo contra los objetivos o metas del mismo (valor mínimo aceptable de cumplimiento vs objetivo),
- Se requiere permitir que los agentes en la Administración de operaciones de seguridad identifiquen claramente la criticidad, el área y Acuerdo de Nivel de Servicios asociado a llamada ó incidente que se este registrando.

#### 6.6.3.6 SOLUCIÓN DE DETECCIÓN Y GESTIÓN DE VULNERABILIDADES:

El ICBF requiere una solución de detección y gestión de vulnerabilidades para los servidores y aplicaciones del ICBF y sobre plataformas suministradas por El Contratista.

Las Características de la solución son:

- Appliance físico.
- La solución debe tener la posibilidad de desplegarse en diferentes redes y segmentos.
- Debe evaluar y gestionar sus vulnerabilidades internas y externas.
- Debe poder ser Implementada de forma rápida.
- Debe identificar vulnerabilidades de dispositivos de red, servidores, estaciones de trabajo y otros dispositivos conectados a la red.
- El alcance para la implementación de la solución de detección y gestión de vulnerabilidades aplica para los servidores declarados en la línea base.
- Los resultados y datos obtenidos en la detección de vulnerabilidades se deben guardar dentro del Appliance, garantizando que los datos nunca salgan de la red interna del ICBF.
- Administración centralizada:
  - Administración del usuario ilimitada y personalizable basada en roles
  - Organización de activos eficaz y flexible
  - Seguimiento de correcciones
  - Escaneado de verificación
  - Entrada con autenticación de 2 factores
- Funcionalidad automatizada:
  - Identificación automática de nuevos activos y evaluación de criticidad
  - Auditoría sin agentes
  - Actualizaciones diarias de comprobaciones de vulnerabilidad
  - Elaboración automatizada de informes y drill down

- Notificaciones sobre nuevas amenazas a través de correo electrónico, sistemas de seguimiento o syslog
- Integración AD para usuarios
- **Análisis:**
  - Creación flexible de informes
  - Informes ajustados a todo tipo de usuario.
  - La clasificación de riesgos CVSS (Sistema de puntuación común de vulnerabilidades) que permita identificar rápidamente los riesgos críticos usando una escala de 1,0-10,0
  - Tablero personalizable y filtros de informes
  - Tendencias sobre grupos de activos y tiempo
  - Informes con todas las soluciones necesarias para resolver problemas
  - Debe encontrar todas las vulnerabilidades atacables remotamente con un filtrado simple

#### **6.6.4 ALMACENAMIENTO**

Para este servicio el ICBF requiere la administración, operación, configuración y monitoreo de las soluciones de almacenamiento SAN y NAS con las que cuenta el ICBF, así como también se requiere de la administración, operación, configuración y monitoreo del nuevo software y hardware que adquiera el ICBF para el mejorar el desempeño del almacenamiento. De igual forma se requiere de la implementación de las recomendaciones y solicitudes realizadas por parte de la Entidad.

#### **6.6.5 RESPALDOS (BACKUP)**

Para este servicio el ICBF requiere la administración, operación, configuración, y monitoreo de las soluciones de respaldo (Networker, Avamar) con las que cuenta el ICBF y las que se adquieran durante la ejecución del contrato. Debido a que el equipo actual de Backup propiedad del ICBF no tiene la suficiente capacidad de Almacenamiento de Backups se debe proporcionar por parte del Contratista el servicio de Backup que satisfaga las necesidades actuales y futuras del ICBF. Este servicio incluye la implementación, actualización y ejecución de las políticas de backup y recuperación para servidores en los diferentes ambientes (desarrollo, pruebas, capacitación, pilotos y producción) y mantener actualizada mensualmente esta información.

De igual forma este servicio contempla el 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.

El Contratista deberá dimensionar la infraestructura necesaria requerida y prestar el adecuado servicio, el cual debe garantizar que no se presenten relanzamientos de Backups por falta de recursos y asegurar en todo momento, mediante soluciones de contingencia, la toma de copias de seguridad íntegras de la información acorde a las programaciones de solicitud de backup, evaluando en caso de ser necesario la provisión de infraestructura o recursos adicionales a los existentes.

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 compatibles con LTO4. Asimismo, deberá evaluarse el reporte automático entre la solución de backup y la herramienta de gestión de servicios.

El servicio de respaldos incluye la custodia de medios y a su vez contiene: almacenamiento, transporte de medios magnéticos, bóvedas especiales, personal capacitado en la manipulación de información y estrictas medidas de seguridad, que permitan garantizar la conservación y seguridad de la información. Los requerimientos mínimos que se debe cumplir con el servicio de custodia externa son:

1. 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 Impermeabilizada: 15°C a 25°C, Humedad Relativa: 40% a 60% y ambiente controlado.
2. Las cintas o medios resguardados deben colocarse en estantes o armarios adecuados en una biblioteca de cintas.
3. 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.
4. 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.
5. Efectuar la marcación de medios magnéticos de acuerdo con la nomenclatura y/o estándar del ICBF.
6. Recibir como mínimo 1 vez a la semana los medios a ser enviados en custodia.

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). Además debe 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.

Actualmente el ICBF está adelantando el proceso de Selección Abreviada por Subasta Inversa Electrónica No. 008 de 2015 con el objeto de “Adquirir solución de respaldo basada en tecnología de discos duros, la ampliación de la solución de Almacenamiento SAN, la garantía extendida 7X24 para las soluciones de almacenamiento SAN, NAS y RESPALDO, Biblioteca de cintas modular (librería) e instalación de la misma.” Con la infraestructura a adquirir se pretende respaldar estaciones de trabajo (Desktop y Laptop) de los usuarios finales por demanda y de manera remota.

#### **6.6.6 OFFICE 365**

El OFERENTE debe cotizar este servicio de la siguiente manera:

##### **NOTA 1:**

- El servicio de Office 365 incluyendo todos los servicios que se enuncian al respecto en el presente capítulo y los perfiles de especialistas correspondientes adjuntos en el Anexo 006 - PERFILES PROFESIONALES REQUERIDOS.
- El servicio de correo electrónico On-Premise (Exchange Server 2010) y El servicio de Lync On-Premise / On-Line 2013 y los perfiles correspondiente a Administrador de plataforma de correo On-Premise y Administrador de Plataforma Lync en el Anexo 006 - PERFILES PROFESIONALES REQUERIDOS

##### **NOTA 2:**

- El servicio de correo electrónico On-Premise (Exchange Server 2010) y El servicio de Lync On-Premise / On-Line 2013 y los perfiles correspondiente a Administrador de plataforma de correo On-Premise y Administrador de Plataforma Lync en el Anexo 006 - PERFILES PROFESIONALES REQUERIDOS

Para este servicio se requiere garantizar la administración, configuración, operación, soporte y monitoreo de la plataforma de Office 365, la cual estará conformada por los servicios e Infraestructura de:

- Servicios de Sincronización y Federación para Office 365
- Lync Server On-Premise (Server 2013)
- Lync Online
- Exchange Online
- Exchange On-Premise (Server 2010)

- SharePoint On-Premise (Server 2013)
- SharePoint Online
- Yammer

Adicionalmente se requiere realizar la gestión del soporte técnico con fabricante, realizar el mantenimiento, migración, upgrade de la infraestructura, sus servicios, componentes y/o unidades lógicas en caso de ser requerido.

Para el servicio específico de correo (Exchange On-Premise / On-Line), para el backup de buzones de correo electrónico El Contratista debe usar las herramientas de retención y descarga que vienen incluidas con la plataforma de Office 365.

Office 365, cuenta con un servicio de administración de dispositivos móviles, El Contratista debe administrar, gestionar y soportar esta herramienta.

Para el servicio de correo electrónico se requiere la administración, configuración, operación, soporte y monitoreo de la plataforma de **correo electrónico On-Premise**, la cual estará conformada por los servicios e Infraestructura de Exchange Server 2010 y realizar la gestión de soporte técnico con el fabricante, componentes y/o unidades lógicas en caso de ser requerido.

El ICBF para el servicio de correo On-Premise requiere:

- La administración del servicio de correo e infraestructura de Exchange Server (On-premise) 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.
- Realizar la gestión del soporte técnico con fabricante, realizar el mantenimiento, migración, upgrade de la infraestructura, sus servicios, componentes y/o unidades lógicas en caso de ser requerido.
- 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.
- Garantizar el acceso a la plataforma OWA (Outlook Web Access) a través de un navegador – servicio web.
- Configurar e implementar las políticas de backup incrementales y totales periódicos de bases de datos de correo.
- 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.

- 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.
- Configurar filtros y redirección de mensajes a carpetas personales o archivados locales en caso de ser requeridos.
- Garantiza la configuración y ajustes de usuarios de Exchange Online acorde con la configuración del servicio del DNS, y Autodiscover de correo.
- Crear y gestionar las listas de distribución, que el ICBF requiera de acuerdo a sus necesidades.
- 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.
- Proporcionar la delegación en la administración de buzones (Superior – subalterno) o retirar los mismos. Los procedimientos deberán establecerse entre El Contratista y el ICBF.
- 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.

Para el servicio de Lync se requiere la administración, configuración, operación, soporte y monitoreo de la plataforma de **correo electrónico On-Premise / On-Line**, la cual estará conformada por los servicios e Infraestructura de Exchange Server 2010 y el servicio de Lync en la Nube. Se deberá realizar la gestión de soporte técnico con el fabricante sobre el servicio, los componentes y unidades lógicas en caso de ser requerido.

El ICBF para el servicio de correo Lync requiere:

- La administración del servicio de Lync On-Premise / On-Line en entorno híbrido (Infraestructura On-Premise y Servicio de Nube) 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.
- Realizar la gestión del soporte técnico con fabricante, realizar el mantenimiento, migración, upgrade de la infraestructura, sus servicios, componentes y/o unidades lógicas en caso de ser requerido.
- 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.
- Configurar e implementar las políticas de backup incrementales y totales periódicos de bases de datos de Lync On-Premise.

- 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.
- Garantizar la operación híbrida entre la Infraestructura On-Premise y el servicio de Nube.
- Activar, Desactivar, Actualizar, Eliminar, Actualizar los usuarios del ICBF en el servicio de Lync de acuerdo a las directrices del ICBF.
- Realizar los ajustes de configuración y requerimientos o incidentes que se generen sobre de la plataforma de Lync en todos sus servicios y funcionalidades bajo los lineamientos destinados para tal fin.

### **6.6.7 APLICACIONES**

En este servicio el ICBF requiere 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 surjan durante la vigencia del contrato (Ver ANEXO 001-LINEA BASE-INFRAESTRUCTURA). Adicionalmente, se requiere realizar el despliegue, emitir recomendaciones de mejores prácticas en configuración y puesta en producción de las aplicaciones que se requieran implementar durante la ejecución 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.

El servicio de aplicaciones incluye la configuración, administración, gestión y monitoreo (7X24X365) las aplicaciones en el ambiente de producción. En caso de que se presenten fallas en el servicio, el CONTRATISTA deberá restablecer el acceso y disponibilidad de las aplicaciones del ICBF de acuerdo a los ANS establecidos.

Para el servicio de aplicaciones el ICBF requiere:

- La configuración de la infraestructura de las aplicaciones.
- La instalación y configuración de parches.
- Suministrar estadísticas de uso y peticiones por aplicación.
- Suministrar información de la utilización real del sistema comparada con las previsiones del Plan de Capacidad.
- Mantener actualizada la arquitectura del servicio.
- 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.

- Proponer, diseñar, administrar, monitorear y configurar esquemas de alta disponibilidad que se requieran para el montaje de Clúster, Network Load Balancing (NLB), balanceo por hardware u otros de similares o mejores características que determine EL CONTRATISTA, utilizando el hardware y el software proporcionado por el ICBF
- La 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.
- Configurar y administrar virtualización de aplicaciones con la herramienta de Citrix (XenApp), el ICBF suministrará el licenciamiento y la infraestructura necesaria.
- Apoyar a la Subdirección de Sistemas Integrados de Información con la solución de incidentes y requerimientos referentes a la arquitectura de software en la operación de los sistemas de información del ICBF.

#### **6.6.8 BASES DE DATOS**

Para las bases de datos el ICBF requiere 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 que soportarán los sistemas de información del ICBF, así como aquellas que se adquieran durante la vigencia del contrato.

El servicio de administración de base de datos incluye el diagnóstico para todas las bases de datos que el ICBF utiliza. Igualmente incluye la presentación de recomendaciones sobre las bases de datos en los diferentes ambientes que se alojen tanto en el Data Center Externo, como en el Centro de Cómputo, las que adquiera durante la vigencia del contrato y las que se migren a la nube de acuerdo al procedimiento interno del ICBF de Puesta en Producción de proyectos de Software.

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.

Para este servicio se requiere que El Contratista proponga, implemente y administre 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 administrar la IaaS en caso de que el ICBF lo requiera. El ICBF proporcionará las licencias necesarias para los motores de bases de datos.

El servicio incluye realizar el montaje, administración, diagnóstico y soporte del motor de base de datos y de componentes tales como reporting services, integration services, analysis services, business Intelligence.

El ICBF necesita que El Contratista analice y realice 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. Es responsabilidad de El Contratista apoyar al ICBF en la validación de la compatibilidad de los aplicativos con las nuevas versiones y ediciones de bases de datos.

Además para el servicio de Bases de Datos el ICBF requiere:

- 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.
- 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 (Recovery Manager).
- Administrar, configurar y automatizar tareas de mantenimiento y optimización de los motores de bases de datos a través de las herramientas propias del motor de base de datos o que El Contratista suministre.
- 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.
- 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 según el procedimiento de control de cambios.
- 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.

- Gestionar y administrar las herramientas de configuración como:
  - 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.
- Gestionar, configurar y administrar las herramientas de rendimiento de MS SQL Server.
- Analizar planes de ejecución (MS SQL Server) sobre consultas con el fin de identificar y corregir cuellos de botella a quien corresponda.
- 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 y dejando como evidencia los logs.
- Gestionar el crecimiento de las bases de datos y diseñar los planes apropiados para administrarlos.
- 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.
- Monitorear las tareas programadas (7X24X365) creadas en los motores de base de datos e informar oportunamente las fallas presentadas emitiendo un diagnóstico y recomendación.
- Monitorear (7X24X365) 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.
- Estandarizar la ubicación física y lógica de las bases de datos en todos los equipos servidores, generando instalaciones de acuerdo a las mejores prácticas recomendadas por los fabricantes de las bases de datos.
- Generar alertas cuando el servicio no esté disponible o se presenten fallas, documentar los incidentes, acciones realizadas y planes de mitigación de riesgos.
- Mantener actualizado el inventario de Base de Datos de acuerdo a los formatos establecidos en conjunto con el ICBF.
- Aplicación continua de las políticas, procedimientos y estándares para la creación, uso, distribución y eliminación de datos en las Base de datos.
- Establecer, documentar e implementar, en conjunto con el ICBF, las políticas de acceso para cada una de las bases de datos.
- 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.
- Diseño, desarrollo, configuración y ejecución de ETL y Cubos sobre las bases de datos de SQL Server.

#### 6.6.9 HERRAMIENTAS DE GESTIÓN, MONITOREO Y SEGURIDAD

El ICBF requiere la gestión, administración y monitoreo con las siguientes herramientas con personal certificado en las mismas:

- Unisphere, Navisphere, Analyser EMC, Thin Provisioning EMC, SAN Copy EMC, SnapView EMC, Fast Suite EMC
- Networker y Avamar para gestión de Backups,
- Microsoft System Center: para los siguientes módulos los cuales deben ser gestionados, administrados y monitoreados en todas sus funcionalidades:
  - Configuration Manager + Endpoint Protection
  - Service Manager
  - Operation Manager
  - Virtual Machine Manager
  - Data Protection Manager
  - Orchestrator

En caso de que la Suite System Center o las herramientas antes expuestas no cumplan algún requerimiento del presente capítulo, El Contratista deberá suministrar las herramientas adicionales que considere necesario para el cumplimiento del presente, previo concepto o 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.

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, Dispositivos Móviles, Equipos de Red, Servidores (físicos y virtuales), Impresoras, Aires Acondicionados (que posean conectividad de red), UPS's, entre otros, que sean propiedad o que estén al servicio del ICBF.

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 anomalía 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 las Subdirecciones de Sistemas integrados de información y la Recursos Tecnológicos para llevar a cabo el seguimiento y control.
- Permitir la distribución de software de manera automatizada a toda la plataforma tecnológica de la red del ICBF (End Points).
- Permitir la gestión, administración y el monitoreo de los Puntos Finales del ICBF.
- 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.
- Permitir la preparación y alistamiento masivo de máquinas.

#### **6.6.9.1 Monitoreo y 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, SystemCenter, y las que el ICBF adquiera para este fin durante el transcurso del Contrato.

El contratista debe mantener la línea base de licenciamiento a través de la herramienta de gestión SystemCenter, por lo cual debe poder retirar las aplicaciones y/o software no autorizado que se encuentre instalado en los equipos que hacen parte del parque computacional de la entidad

Para los casos en que el ICBF adquiera licencias de uso de un software se podrá requerir la configuración de la herramienta para la realización de despliegues masivos de instalación de software mencionado.

El contratista debe remitir informes mensuales donde se evidencie la gestión de licenciamiento:

- Software instalado por máquina
- Manejo de listas negras del licenciamiento
- Resultados del cruce de software adquirido vrs. el licenciamiento instalado
- Uso de software licenciado por equipo.

#### 6.6.9.2 Monitoreo De 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
  - Peticiones recibidas por segundo
  - Publica solicitudes por segundo
  - Máximo de conexiones
    - Not Found (404) Error por segundo
    - Porcentaje de tiempo de procesador
    - Caché porcentaje Hit
    - Solicitud de 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.

#### 6.6.9.3 Monitoreo De Base De Datos

##### Bases de Datos Oracle:

- 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 procesos 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.

#### **Bases de Datos 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.

#### Bases de Datos 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 coleccionar 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 coleccionadas.

#### 6.6.9.4 Monitoreo De 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 procesador time
  - Windows/Processor queue length
  - Windows/Carga de transacciones
  - Windows/Disk time
  - Windows/Disk queue length
  - Windows/Page Fault/sec
  - Windows/Pages/sec
  - Windows/Pool Nonpaged bytes
  - Windows/Paginación
  - Windows/Procesos de S.O. críticos (Lsass, Svchost, Ntfs)
  - 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.

#### **6.6.10 REDES DE AREA LOCAL (LAN)**

El servicio de RED LAN debe permitir a los funcionarios del ICBF de la sede de la Dirección General y sedes Anexas la conectividad a periféricos de salida como impresoras, escáneres y transferencia de datos localmente entre dispositivos y endpoints, a través de la interconexión de dispositivos activos como switches y access point, los cuales se relacionan en el *Anexo 008 - EQUIPOS - RED LAN -WLAN*. El alcance de El Contratista será llegar al Rack de Comunicaciones de cada área de la Sede de la Dirección General y de las sedes anexas y administrar, operar y monitorear los dispositivos de red necesarios para garantizar el servicio. Adicionalmente se requiere la instalación de nuevos switches cuando sea requerido para mejorar el desempeño de

la red o cuando fallen y se requiera el reemplazo de los mismos. Estos dispositivos serán entregados por el ICBF al Contratista para dicha instalación y configuración.

El cableado estructurado para interconexión de equipos en el interior de las sedes será responsabilidad del ICBF.

Además para el servicio de administración de Red LAN se requiere como mínimo las siguientes actividades:

- Monitorear permanentemente la red DE AREA LOCAL (LAN), permitiendo conocer en tiempo real el desempeño y la disponibilidad de los equipos que conforman la red y sus componentes asociados (Management Information Base -MIB). Las variables mínimo a monitorear son: Fuente de Poder, Ventilador, Procesador, Memoria, Puertos, Disponibilidad del Equipo.
- Administrar el direccionamiento IP asignación de direcciones dual Stack IPv4 e IPv6 a los equipos y dispositivos de acuerdo a las mejores prácticas.
- Instalar y configurar el hardware y software necesario para el buen funcionamiento y servicio de la red LAN, incluido la realización de respaldo de configuración y actualización de firmware de los equipos que están relacionados en el Anexo 008 - EQUIPOS - RED LAN -WLAN y los equipos que se adquieran o cambien durante la vigencia del contrato. La información de la configuración de los switches de acceso y switch core debe estar respaldada en la unidad de almacenamiento que el ICBF disponga.
- Crear nuevas redes, subredes, VLANS y rutas de acuerdo a las necesidades en la infraestructura del ICBF.
- Realizar el diagnóstico para el mejoramiento y ampliación de la red LAN, con el fin de incluir nuevos servicios respondiendo a las necesidades de crecimiento del ICBF.
- Realizar el mapeo de la Red LAN de la sede de la Dirección General y Sedes Anexas, donde se indique por medio de un diagrama todos los puertos de los switches y de estos cuales se encuentran ocupados y libres, que dispositivo se encuentra instalado y su ubicación. Este mapeo debe estar actualizado ante cualquier cambio realizado.
- Configurar en los equipos relacionados en el Anexo 008 - EQUIPOS - RED LAN -WLAN el protocolo SSH (Secure SHell) y deshabilitar el acceso remoto por Web y por Telnet con el propósito de ofrecer mayor seguridad a la red.
- Realizar la tareas necesarias para segmentar la red LAN de las sede de la Dirección General y sede Anexas, según los parámetro definidos por el ICBF.

- Bloquear y desbloquear puertos de conexión según los requerimientos del ICBF.
- Implementación de un servidor TACAS (Terminal Access Controller Access Control System) o RADIUS (Remote Authentication Dial-In User Service) para el ingreso a la configuración de los switches únicamente al personal autorizado por el ICBF.

#### **6.6.11 REDES INALAMBRICAS (WLAN)**

El ICBF requiere la configuración, administración y soporte del servicio WLAN y los componentes que permiten su funcionamiento para las sedes del ICBF descritas en el Anexo 008 - EQUIPOS - RED LAN -WLAN. Para los Access point marca Aerohive AP-230 El Contratista debe administrar los equipos a través de un controlador con interfaz web en el portal del fabricante. Para los access point marca HP MS-430, El Contratista debe realizar la administración a través de la interfaz que estos equipos suministran localmente.

Se requiere la administración de los Access Points y de los Controladores de Acceso de la RED INALAMBRICA sin importar su ubicación física dentro de las sedes del alcance de este servicio.

Dentro del servicio y administración se deben garantizar lo siguiente:

- Aplicar políticas de QoS, Seguridad y cobertura (RF) a los Access Points por medio de los Controladores de Puntos de Acceso Distribuidos por la red la RED INALAMBRICA.
- Integrar planos pre configurados en la herramienta de administración.
- Visualización de Heat Maps y cobertura en radio frecuencia
- Permitir la localización de los Access Points y clientes WiFi que se encuentren en la red INALAMBRICA (WLAN) mediante planos preconfigurados, incluidos los equipos móviles.
- Consolidar alarmas y reportes de los niveles de radio, interferencia, seguridad, desempeño.
- Incluir herramientas para planificación del crecimiento de la red Wireless, mostrando los sitios más indicados para la instalación de nuevos Puntos de Acceso.
- Implementar IDS (Intrusion Detection System) basado en firmas de radio frecuencia (RF)
- Instalar Access point cuando se requiera para ampliación según el mapa de calor o cuando fallen los dispositivos.

#### **6.6.12 INTERNET MOVIL**

El Contratista deberá suministrar el servicio de internet móvil dentro de los 15 días calendario siguiente a la firma del contrato, la velocidad de los planes debe garantizar el normal funcionamiento de todas las aplicaciones y servicios incluido el acceso por medio de VPN.

El supervisor del contrato o quien este delegue, remitirá al contratista vía correo electrónico la solicitud de activación de los módems, una vez estos hayan sido distribuidos.

Los módems y MIFI serán utilizados por funcionarios del ICBF a partir de la fecha de solicitud de activación y hasta cuando el ICBF solicite la cancelación del uso del equipo o cuando termine el periodo de ejecución del contrato. Estos deberán tener cobertura a nivel nacional para la cual el ICBF designe su uso y un horario de funcionamiento 7X24X365.

El Contratista deberá entregar los módems y MIFI sin activar el servicio de internet móvil y realizar la distribución de los mismos según requerimientos determinados por la Entidad y el informe de cobertura presentado por El Contratista.

. Una vez se suministren los módems y MIFI estos deben estar bloqueados para contratar o adquirir servicios diferentes a los aquí señalados, a fin de evitar la generación de sobrecostos por envío de mensajes de textos, suscripción a otros servicios, o cualquier actividad que genere un costo adicional.

### **6.6.13 GOBERNABILIDAD**

La estructura organizacional del ICBF se encuentra detallada en el siguiente enlace:

<http://www.icbf.gov.co/portal/page/portal/Intranet/ICBF/organigrama>

Este organigrama servirá de guía para entender la estructura organizacional y dinámica del ICBF que debe ser tomada en cuenta para el dimensionamiento que se exponga en el presente capítulo y para la efectiva gestión de todos los servicios.

#### **6.6.13.1 Organización Del Proyecto**

A continuación se mencionan los Stakeholders relacionados para el presente 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, dentro del alcance del contrato, 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.

#### 6.6.13.2 Roles

Para la ejecución del contrato la SRT se encuentra conformada por Ingenieros a cargo de los diferentes servicios que permitirán dirigir y coordinar la labor realizada por el personal del Contratista asignado para el contrato, 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 del Contratista a través del Subdirector de Recursos Tecnológicos 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 revisión 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 y Soporte en Sitio:** Es el responsable de la ejecución del contrato de Mesa de Servicio y Soporte en Sitio - UNION TEMPORAL GESTION INTEGRAL MESA ICBF - 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 Conectividad:** 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) e internet del ICBF.

**EL CONTRATISTA de Housign Y Nube Privada:** Es el responsable de la ejecución del contrato de Housign Y Nube Privada suscrito con el ICBF y en el cual existen servicios que se interrelaciona con el presente contrato, tales como servidores en nube privada, appliance de seguridad, rack y conexiones eléctricas y de red en modalidad de housing.

**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. Los roles para cada proceso de ITIL descrito a continuación se requieren con la dedicación descrita en el ANEXO 006 PERFILES PROFESIONALES REQUERIDOS y deberán contar con el conocimiento y experiencia en ITIL v.3 o superior.

El rol de Gestor de Cambios debe desempeñarse en forma exclusiva, tiempo completo y no debe asumir roles que hagan parte de la operación.

Dichos roles son:

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

EL CONTRATISTA deberá permanecer en constante comunicación con los tres proveedores de servicios adicionales (Conectividad, Housign y Nube Privada y Mesa de Servicios y Soporte en Sitio) 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 cuatro 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.

### 6.6.13.3 Comités

El ICBF requiere que se conformen 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 de ICBF.

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

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; como también para 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, el coordinador de operaciones 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 y Gestiones ITIL:** Estas mesas están conformadas por el líder del servicio tanto del ICBF como los especialistas 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 lineamientos, 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 **CONECTIVIDAD – INFRAESTRUCTURA – MESA DE SERVICIO Y SOPORTE EN SITIO**, este comité generara compromiso que serán de obligatorio cumplimiento para todos los contratos previa aprobación del Supervisor.

#### 6.6.13.4 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 Dirección de proyecto: 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.

- Los planes y documentos relacionados en el **Anexo 005 – Matriz chequeo organización del proyecto** serán solicitados previo acuerdo entre el Supervisor y Contratista.

#### 6.6.13.5 Equipo De Trabajo Del ICBF

Es el equipo del ICBF conformado por el Gerente del proyecto, los Ingenieros Líderes del servicio, los profesionales encargados del seguimiento contractual, financiero, jurídico y administrativo los cuales participan en la ejecución del proyecto y realizarán las siguientes actividades:

- Mantener una continua y adecuada disponibilidad para atender y resolver oportunamente los inconvenientes que se puedan presentar durante la Etapa de Operación del proyecto.
- Discutir, revisar y aprobar los planes de contingencia propuestos por El Contratista que garanticen la continuidad en los servicios, según las necesidades y prioridades definidas por el ICBF.
- Discutir, revisar y aprobar los planes de mejoramiento propuestos por El Contratista que garanticen la prestación con calidad de los servicios, según las necesidades y prioridades definidas por el ICBF.
- Verificar el cumplimiento de los aspectos contractuales y otros acuerdos pactados con El Contratista.
- Coordinar y facilitar las actividades por parte del ICBF necesarias para la prestación del servicio por parte de El Contratista.
- Informar y divulgar el alcance de los servicios prestados por El Contratista al interior del ICBF.
- Detectar oportunamente las necesidades de las diferentes áreas del ICBF, relacionadas con la prestación de los servicios y realizar propuestas que permitan la solución a estas necesidades.
- Mantener informado al Gerente del proyecto designado por el ICBF los aspectos relacionados con la prestación del servicio y entregar los informes y registros de actividades solicitados.
- Informar oportunamente al SUPERVISOR del contrato, sobre eventos que afecten la correcta ejecución del contrato como son: incumplimientos, anomalías, inconformidades o deficiencias presentadas por EL CONTRATISTA en la prestación del servicio y obligaciones contractuales.
- Coordinar actividades enfocadas a fortalecer valores tales como confiabilidad e integridad, entre los entes involucrados en el contrato.

- Realizar seguimiento y verificación del servicio prestado por EL CONTRATISTA con el fin de asegurar la calidad del mismo, realizando visitas esporádicas a cualquier sede que este atendida por El Contratista.
- Verificar y aprobar informes entregados por EL CONTRATISTA.
- Verificar el cumplimiento de los ANS y generar las penalizaciones a que haya lugar.
- Verificar la liquidación de los servicios para la facturación que presenta EL CONTRATISTA.
- Realizar el seguimiento financiero a la ejecución del contrato.
- Gestionar y tramitar los pagos correspondientes.
- Proyectar comunicados oficiales dirigidos a EL CONTRATISTA.
- Realizar los informes de seguimiento del contrato.

Nota: Para cada uno de los servicios anteriormente descritos se requiere que en la herramienta de gestión de mesa de servicio que disponga el ICBF se gestione y documente los tickets que por incidentes, requerimientos y controles de cambios se generen.

#### 6.6.13.6 Elementos de Comunicación

El Contratista deberá suministrar al Supervisor del Contrato máximo en los primeros 15 (quince) días del contrato, 14 (Catorce) Smartphones que soporten última tecnología (4g o superior) pantalla táctil, resolución 640 X 1080 pixeles, memoria interna de mínimo 16 GB, autonomía de batería en conversación mínimo 12 horas, conectividad Redes móviles e inalámbricas WiFi, Bluetooth 4.0 o equivalentes, que permita la utilización de los servicios de Office 365 (Correo, Lync, OneDrive, Yammer, Office Mobile), Skype, Cámara trasera y frontal, con planes de voz de mínimo 1.000 minutos mensuales a cualquier operador telefónico nacional, plan cerrado (no debe permitir exceder los minutos al mes asignado) y Plan de Datos de Internet Ilimitado, estos serán utilizados por los profesionales de la SRT que tienen que realizar gestión y el seguimiento al cumplimiento de las actividades diarias y apoyar la coordinación con el personal de la Subdirección de Recursos Tecnológicos y de los Operadores de TIC, dicho seguimiento corresponde a los servicios (Aplicaciones, Bases de Datos, Seguridad Informática, Redes, Correo Electrónico, Backup, Almacenamiento, Datacenter, Servidores, Gestión de Cambios, y demás servicios o roles que participen y tengan objeto dentro del presente contrato), y que deben estar en todo momento en contacto con El Contratista y demás operadores de TIC. Todos los elementos que se entreguen al servicio de este contrato (Hardware, Software, Teléfonos, entre otros) únicamente serán asignados para el objeto y el cumplimiento del contrato.

## 7. OBLIGACIONES DEL CONTRATISTA

## **7.1 Obligaciones específicas**

EL CONTRATISTA se obliga a garantizar el cumplimiento de los servicios ofertados, que deben ser como mínimo los requeridos por el ICBF. Para los servicios descritos en este documento EL CONTRATISTA deberá:

### **Centros de Cómputo**

- 7.1.1. Administrar y monitorear 7X24X365 la operación de la infraestructura del Centro de Cómputo de la Sede de la Dirección General.
- 7.1.2. 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.
- 7.1.3. 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.
- 7.1.4. Diseñar, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de Centro de Cómputo de la SEDE DE LA DIRECCIÓN GENERAL.
- 7.1.5. 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 ser arreglado o reemplazado en forma inmediata por EL CONTRATISTA con el fin de normalizar la operación.

- 7.1.6. Acompañar al personal técnico que adelanta trabajos (cualquier actividad) en el Centro de Cómputo del ICBF durante el desarrollo de su labor, previa comunicación del ICBF al EL CONTRATISTA.
- 7.1.7. 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.
  - Sistema de detección de incendios.
  - Sistema eléctrico regulado UPS 30 kva
  - Control de seguridad física (seguridad perimetral, sistemas de vigilancia, sistemas de control de accesos).
  - Circuito cerrado de televisión (CCTV).

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

- 7.1.8. 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
  - Control de acceso biométrico
  - Sistema eléctrico regulado y no regulado (tableros eléctricos) incluyendo sus componentes.
  - Sistema eléctrico regulado UPS 30 kva.
- 7.1.9. 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.
    - Transformador de aislamiento
    - Gestión de alarmas.

- Control de seguridad (seguridad perimetral, sistemas de vigilancia, sistemas de control de accesos).
- Sistema eléctrico regulado UPS 30 kva
- Topología del Data Center Externo y Centro de Cómputo

7.1.10. 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.

## **Servidores**

### **Servicio de Administración y operación**

- 7.1.11. 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.
- 7.1.12. 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.
- 7.1.13. Verificar las bitácoras de errores, problemas y logs para búsqueda de causas de incidentes ocurridos y/o para prevenir su ocurrencia.
- 7.1.14. Instalar, configurar, administrar y monitorear nuevo hardware y software para servidores que entre en operación durante el contrato, cuando el ICBF así lo requiera.
- 7.1.15. Realizar la instalación, configuración, administración y monitoreo a nivel de servidores, de servicios de escritorio como servicios de Impresión y scanning, políticas y demás publicados en Directorio Activo.
- 7.1.16. Generar un plan para realizar la aplicación de actualizaciones a firmware, fixes y 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.

- 7.1.17. 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.
- 7.1.18. Realizar la marcación de los servidores físicos de acuerdo a los lineamientos dados por el ICBF.
- 7.1.19. 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.
- 7.1.20. Generar informe bimestral con la lista de servidores sin utilizar en un período igual o mayor a 3 meses.
- 7.1.21. Configurar en todos los servidores objetos de monitoreo los agentes necesarios para la notificación en la herramienta de gestión que se encuentre en operación en el ICBF para la apertura de tickets.
- 7.1.22. 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.
- 7.1.23. Diseñar, crear, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de Servidores.
- 7.1.24. Analizar, diseñar, proponer y ejecutar las configuraciones y arreglos de servidores necesarios para dotar de alta disponibilidad la plataforma de clusterización de servidores.
- 7.1.25. Cuando el ICBF lo requiera EL CONTRATISTA debe instalar, configurar, administrar, monitorear y/o brindar apoyo a los proveedores sobre el nuevo hardware de servidores y software que entre en operación durante el contrato.
- 7.1.26. Analizar, diseñar, proponer y ejecutar las configuraciones necesarias previa verificación del ICBF de nuevos sistemas que optimicen procedimientos.
- 7.1.27. Generar los mapas lógicos de interconexión de servidores de aplicaciones y base de datos y mantenerlos actualizados.
- 7.1.28. 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.

- 7.1.29. Documentar cada ticket en la herramienta que disponga el ICBF (llamada de servicio, incidente o problema) relacionado con fallos en los servidores. Dar apoyo en el diagnóstico de las causas de los mismos, independientemente del ambiente del servidor (Piloto, Desarrollo, Pruebas, Producción) y presentar el informe respectivo.
- 7.1.30. 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 CMDDB actualizada. Además mantendrá actualizadas las hojas de vidas de los servidores en un formato diseñado para ello en conjunto y presentarlas al ICBF cuando este lo requiera
- 7.1.31. 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 24 Horas siguientes al incidente.
- 7.1.32. Cuando se presente una falla en los servidores y no sea posible la solución remota, El Contratista deberá desplazarse a los DataCenter y dar soporte en sitio.

#### **Controladores de Dominio (DC)**

- 7.1.33. Administrar las herramientas para el manejo de bases de datos de Directorio Activo, DNS, DHCP.
- 7.1.34. Realizar las recomendaciones necesarias para que el sistema de Directorio Activo, DHCP y DNS funcione de la manera más adecuada.
- 7.1.35. 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).
- 7.1.36. 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).

- 7.1.37. Controlar y monitorear la frecuencia en fallos de autenticación de red (bloqueo) mediante el uso de una herramienta que permita el cambio automático de claves por olvido de la misma.
- 7.1.38. Controlar y monitorear la frecuencia de expiración y bloqueos por inactividad de cuentas de usuarios.
- 7.1.39. Analizar, diseñar, proponer y ejecutar las configuraciones necesarias para el óptimo funcionamiento del Directorio Activo, DNS y DHCP, previa verificación del ICBF.
- 7.1.40. Realizar las configuraciones necesarias para asegurar la conectividad entre los servidores y los equipos activos de red de los centros de cómputo tanto del ICBF como Externos.
- 7.1.41. Monitorear y soportar la conectividad entre los servidores y los equipos activos de red de los centros de cómputo tanto del ICBF como Externos, y debe solucionar cualquier incidente que afecte la conectividad entre los servidores y los equipos activos de red de los data centers del ICBF y externos que estén al servicio de la operación del ICBF.

#### **SOC ( Security Operation Center)**

Servicio de monitoreo para una Gestión integrada de seguridad, operaciones y riesgos de TI en la plataforma tecnológica instalada en el ICBF

- 7.1.42. El Contratista deberá presentar el plan de trabajo, especificando etapas, resultados esperados, estrategias para asegurar el logro de los productos en los tiempos establecidos y describir las técnicas y herramientas que utilizará en la ejecución del contrato, previa aprobación del ICBF.
- 7.1.43. Garantizar el servicio de monitoreo de la gestión integrada de seguridad compuesto por :
  - Gestión de Bitácoras y Correlación de Eventos de Seguridad en Tiempo Real
  - Gestión de Incidentes en Tiempo Real
  - Gestión de Configuraciones en Tiempo Real
  - Administración de redes en tiempo real
- 7.1.44. Administrar y monitorear 7X24X365 la gestión integrada de seguridad del ICBF.
- 7.1.45. Proporcionar dentro del servicio la capacidad de verificar el cumplimiento de regulaciones y estándares internacionales y nacionales de los dispositivos monitoreados tales como (PCI DSS, SOX, 052, entre otras)

- 7.1.46. Proporcionar el mantenimiento de hardware y actualizaciones de software (parches y upgrades de versión) por la duración del contrato.
- 7.1.47. Proporcionar Soporte técnico del fabricante con atención 8x5 por la duración del contrato.
- 7.1.48. La solución de correlación de eventos deberá contar con un servicio de suscripción para la actualización de contenidos de seguridad, que permitan mantener actualizadas las definiciones de ataques, vulnerabilidades y categorización de eventos durante la vigencia del contrato.
- 7.1.49. Garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el fabricante para una oportuna solución de la solución implementada para la prestación del servicio
- 7.1.50. Proporcionar entrenamiento sobre la solución implementada para la prestación del servicio a nivel administrador y usuario final.

## **Seguridad Perimetral**

### **Servicios de administración y operación de Seguridad Perimetral:**

- 7.1.51. 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.
- 7.1.52. 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.
- 7.1.53. 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.

- 7.1.54. Brindar apoyo técnico y proponer activamente recomendaciones al ICBF tendientes a incrementar el nivel de seguridad informática y al mejoramiento de la 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.
- 7.1.55. 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.
- 7.1.56. 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.
- 7.1.57. Suministrar, instalar, configurar, afinar, monitorear y dar soporte a toda la tecnología necesaria para cubrir los requerimientos técnicos de seguridad descritos en este documento.
- 7.1.58. Capacitar al personal con el fin de que se cumplan todas con las normas y políticas de seguridad del ICBF.
- 7.1.59. Notificar al ICBF, a través del líder de Seguridad, cualquier incidente ocurrido sobre la infraestructura tecnológica.
- 7.1.60. Realizar acciones de respuesta a incidentes de seguridad, en coordinación con el ICBF a través del Líder de Seguridad Informática. Para ello, deberá generar mejoras al procedimiento de gestión de incidentes, un plan de respuesta que conlleve a su solución, asumirá la investigación forense (la infraestructura administrada, suministrada y alojada en el data center, centro de cómputo de la sede Nacional y sedes Regionales, adicionalmente deberá realizar investigación forense a los equipos de cómputo del parque computacional del ICBF cuando se presente un incidente de seguridad) 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.
- 7.1.61. Retener y almacenar los logs relacionados con seguridad por un periodo mínimo de 1 año.

- 7.1.62. 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.
- 7.1.63. 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.
- 7.1.64. 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.
- 7.1.65. Identificar, diagnosticar, solucionar y reportar problemas e incidentes de seguridad en la infraestructura tecnológica del ICBF o la que provea el CONTRATISTA. 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.
- 7.1.66. 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.
- 7.1.67. Definir parámetros técnicos de seguridad en servidores WEB, aplicaciones y servicios en internet para prevenir ataques a la disponibilidad, confidencialidad e integridad de la información de ICBF.
- 7.1.68. 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.

- 7.1.69. 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 y un (1) Certificado tipo SSL SAN Geo Trust para correo Lync 2010 o el equivalente para la versión de Lync 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 014 - INVENTARIO DE CERTIFICADOS DIGITALES**. 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.
- 7.1.70. El Contratista deberá renovar en caso de ser necesario, los certificados digitales públicos o privados necesarios para el debido funcionamiento de todos los servicios del presente contrato.
- 7.1.71. 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.
- 7.1.72. Realizar 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 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.

7.1.73. Diseñar el análisis de riesgos asociado a la infraestructura que disponga para la adecuada prestación de los servicios.

7.1.74. Realizar acompañamiento en la implementación, mantenimiento y operación el SGSI del ICBF.

#### **Antivirus**

7.1.75. Será deber de EL CONTRATISTA administrar y soportar las soluciones de antivirus que el ICBF tenga a disposición.

7.1.76. El Contratista deberá garantizar el despliegue y actualización del Antivirus que se tenga en producción, e informar quincenalmente el estado general de actualización y amenazas detectadas por el mismo.

#### **Firewall de Nueva Generación, IPS/IDS, VPN**

7.1.77. Diseñar la solución de firewall siempre y cuando cumpla con los requerimientos del ICBF descritos en este documento. Dicha solución debe abarcar un firewall perimetral y firewall interno 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.

7.1.78. 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.

- 7.1.79. Realizar la administración, mantenimiento y actualización de los equipos de hardware que conformen la solución de firewall.
- 7.1.80. Otorgar, administrar, gestionar y brindar soporte a los accesos a través de conexiones VPN tanto host to site como site to site.
- 7.1.81. 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 documento. Los controles de acceso lógicos deben estar asociados a Directorio Activo de Microsoft y deben cumplir con la política de 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.
- 7.1.82. 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.
- 7.1.83. Suministrar y administrar herramientas de monitoreo para los firewall de seguridad perimetral, la cual debe estar integrada directamente a la herramienta suministrada para facilitar labores de correlación de eventos y permitir gestión y administración centralizada.
- 7.1.84. 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.

### **Servidor Proxy y Proxy Reverso**

- 7.1.85. Suministrar, instalar y operar una solución proxy en alta disponibilidad para proveer conexión a Internet controlada por políticas de acuerdo a las categorías de navegación disponibles en el mercado.
- 7.1.86. La solución debe permitir crear listas negras y listas blancas de navegación.
- 7.1.87. La solución debe contar con una base de datos de actualización automática para determinar la fiabilidad de los sitios web visitados.
- 7.1.88. La solución debe permitir determinar qué tipos de archivos se pueden descargar al interior de la Entidad.

- 7.1.89. El acceso a los sitios web debe ser administrados por grupos desde directorio activo de Windows.
- 7.1.90. La solución debe permitir realizar traza de navegación por usuario, por categoría y por direccionamiento IP.
- 7.1.91. La autenticación debe ser posible por usuario de dominio ICBF o por direccionamiento IP.
- 7.1.92. Debe permitir el control de aplicaciones de acuerdo a la base de datos del fabricante.
- 7.1.93. Debe permitir la apertura de puertos de navegación.
- 7.1.94. La solución debe conservar el contenido solicitado por el usuario para acelerar la respuesta en futuras peticiones de la misma información de la misma máquina u otras.
- 7.1.95. Integrar las soluciones proxy y control de contenido con los sistemas de autenticación del ICBF como el directorio activo.
- 7.1.96. 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.
- 7.1.97. Realizar la administración, mantenimiento, centralización y actualización de las políticas del filtro de navegación.
- 7.1.98. Suministrar la solución de proxy reverso, de acuerdo a las especificaciones que se impartan desde ICBF

## **DMZ**

- 7.1.99. Realizar planes para la migración de servidores y aplicaciones a la DMZ, de común acuerdo y bajo aprobación del ICBF.
- 7.1.100. Apoyar y realizar las labores técnicas necesarias para migrar servidores y aplicaciones a la DMZ.
- 7.1.101. Alinearse a las políticas de cambios y SGSI implementadas en el ICBF para realizar cualquier configuración o modificación sobre la DMZ.
- 7.1.102. Realizar labores de configuración y soporte para mantener la DMZ en operación.
- 7.1.103. 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.

## **Almacenamiento**

### **Servicios de Administración y operación**

- 7.1.104. 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.
- 7.1.105. Monitorear 7X24X365 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.
- 7.1.106. Apoyar técnicamente 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.
- 7.1.107. Presentar mensualmente los siguientes reportes de comportamiento de la data basados en la herramienta Unisphere, Navisphere y Analyzer: Comportamiento de WorkLoad, Distribución de WorkLoad, Medición a nivel de LUN, Medición a nivel de METALUN, Medición a nivel de StorageProcesor.
- 7.1.108. Apoyar técnicamente en la implementación de soluciones nuevas relacionadas con el servicio y aquellas que adquiera el ICBF.
- 7.1.109. Administrar las herramientas:
- Unisphere
  - Navisphere
  - Analyser EMC
  - Thin Provisioning EMC
  - SAN Copy EMC
  - SnapView EMC
  - Fast Suite EMC.

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.

## **Respaldos (Backup)**

### **Servicios de Administración y operación**

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

- 7.1.111. Prestar el servicio de Backup de acuerdo a las políticas y el dimensionamiento que requiera el ICBF durante la ejecución del CONTRATO.
- 7.1.112. 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.
- 7.1.113. Realizará el monitoreo 7X24X365 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.
- 7.1.114. Desarrollar las actividades relacionadas con respaldo (backup) y restauración (restore) dejando registradas las acciones realizadas en la herramienta de gestión suministrada por el ICBF.
- 7.1.115. Realizar, en coordinación con el servicio de administración de aplicaciones, el levantamiento de aplicativos y bases de datos a nivel nacional, para determinar con los diferentes responsables la pertinencia de la creación, modificación o eliminación de las políticas de respaldo asociadas a estas.
- 7.1.116. 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, de acuerdo a las políticas de Backup vigentes en el ICBF.
- 7.1.117. 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.
- 7.1.118. 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.
- 7.1.119. 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.

- 7.1.120. Suministrar las cintas requeridas (estimadas en 300 anuales) para realizar tareas de backup, las cuales deberán ser proporcionadas desde el inicio del contrato.
- 7.1.121. Mantener actualizada, en documentación previamente concertada con el ICBF, la información correspondiente como mínimo de:
- Inventario de medios
  - Políticas de backup
  - Información respaldada
  - Consumo de medios de respaldo
- 7.1.122. Realizar por lo menos 1 vez por semestre, 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 y se presentarán en el informe del respectivo mes.
- 7.1.123. 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.
- 7.1.124. Cumplir con la norma ISO27001 relacionada al servicio de respaldos.
- 7.1.125. Prestar el servicio de Backup con la herramienta Networker de EMC, 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.
- 7.1.126. Proveer la infraestructura necesaria que garantice la realización de las restauraciones solicitados sin que afecten la realización de los respaldos requeridos.
- 7.1.127. Tener presente 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.

### **Servicios de custodia de medios**

- 7.1.128. Proveer y mantener vigente durante la duración del presente contrato el servicio de custodia de medios que cuenten con: almacenamiento, transporte de medios magnéticos, bóvedas especiales, personal capacitado en la manipulación de

información y estrictas medidas de seguridad, que permitan garantizar la conservación y seguridad de la información.

- 7.1.129. Informar al líder del servicio del ICBF 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.

### **Office 365**

- 7.1.130. 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.
- 7.1.131. 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.
- 7.1.132. Garantizar el acceso a la plataforma OWA (Outlook Web Access) a través de un navegador – servicio web.
- 7.1.133. .
- 7.1.134. Gestionar y Administrar la plataforma de Administración de dispositivos móviles de Office 365.

### **Servicios en General**

- 7.1.135. Realizar la gestión del soporte técnico con fabricante, realizar el mantenimiento, migración, upgrade de la infraestructura, sus servicios, componentes y/o unidades lógicas en caso de ser requerido.
- 7.1.136. Garantizar la administración, gestión, configuración, operación, monitoreo y control de los servicios en el presente de Office 365.
- 7.1.137. Realizar Migración en caso de ser requerida de toda la infraestructura que forma parte de los servicios de Office 365 en el presente y sus respectivas unidades 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.

- 7.1.138. 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.
- 7.1.139. Generar los mecanismos necesarios para el monitoreo de la infraestructura de Office 365.
- 7.1.140. Informar quincenalmente al ICBF el estado de los servicios de Office 365 (Online-Onpremise) 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.
- 7.1.141. 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.
- 7.1.142. Brindar acceso pertinente a los distintos módulos, y/o via Powershell al ICBF, para consultar o auditar los distintos servicios.
- 7.1.143. Gestionar y documentar los incidentes, Cambios, Requerimientos, Problemas en la herramienta definida por el ICBF con la información pertinente, en los tiempos establecidos.
- 7.1.144. Entregar los logs o evidencias requeridas por el ICBF, para cualquiera de los servicios de Office 365 contenidos en el presente documento.
- 7.1.145. Programar, ejecutar y documentar procesos de Microsoft Help Check, de todos los roles y parámetros que conforman la Infraestructura On-premise y Online de todos los servicios de Office 365 una vez al año.
- 7.1.146. 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.

- 7.1.147. 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.
- 7.1.148. 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.
- 7.1.149. 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.
- 7.1.150. Activar, Desactivar, Actualizar, Eliminar, Actualizar los usuarios del ICBF en los servicios de Office 365 (On line – On Premise) de acuerdo a las directrices del ICBF.
- 7.1.151. Realizar los ajustes de configuración, requerimientos o incidentes que se generen sobre de la plataforma de Office 365 (On line – On Premise) en todos sus servicios y funcionalidades bajo los lineamientos destinados para tal fin.

### **Servicios de Sincronización y Federación para Office 365**

- 7.1.152. 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)**

- 7.1.153. Administrar el 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.
- 7.1.154. 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. Este servicio debe proveerse por demanda.

- 7.1.155. 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.
- 7.1.156. 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.
- 7.1.157. Configurar filtros y redirección de mensajes a carpetas personales o archivados locales en caso de ser requeridos.
- 7.1.158. Garantiza la configuración y ajustes de usuarios de Exchange Online acorde con la configuración del servicio del DNS y Autodiscover de correo.
- 7.1.159. Crear y gestionar las listas de distribución que el ICBF requiera de acuerdo a sus necesidades.
- 7.1.160. Proporcionar la delegación en la administración de buzones (Superior – subalterno) o retirar los mismos. Los procedimientos deberán establecerse entre EL CONTRATISTA y el ICBF.
- 7.1.161. 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.
- 7.1.162. Administrar, gestionar, configurar, monitorear y soportar la herramienta EOP (Exchange Online Protection) 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.
- 7.1.163. 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.
- 7.1.164. Realizar los respectivos Backups de Buzones cuando las mismas expiren o se solicite explícitamente por el ICBF a través de la Mesa de Servicio o cuando apliquen los respectivos lineamientos para el tema.

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

- 7.1.165. 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.
- 7.1.166. Administrar la infraestructura On-premise, y los servicios Online que el ICBF tiene destinados para el servicio de LYNC.
- 7.1.167. Garantizar el acceso a través de Internet al servicio de Lync fuera del dominio ICBF.

### **Servicio SharePoint (On-premise – Online)**

- 7.1.168. Realizar la creación, modificación, administración de sitios y subsitios otorgando los permisos que requiera el ICBF, acordes al organigrama del instituto, o a los sitios/subsitios que se autoricen por parte del ICBF.
- 7.1.169. Administrar la Infraestructura On-premise y los servicios de nube pertenecientes al ICBF para la operación de este servicio.
- 7.1.170. 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**

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

## **Aplicaciones**

### **Servicios de Administración y operación**

- 7.1.172. 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.
- 7.1.173. Proponer, diseñar configurar y administrar esquemas de alta disponibilidad y balanceo que soporten las aplicaciones existentes o nuevas del ICBF. El ICBF suministrará Hardware y licencias necesarias.
- 7.1.174. Proponer e implementar soluciones y mejores prácticas de manera eficiente, efectiva y eficaz, trabajando en equipo con la Dirección de Información y Tecnología (DIT).
- 7.1.175. 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, dichos informes se deben entregar en formato digital enviado por correo.
- 7.1.176. Cumplir con las tareas y solicitudes en los tiempos establecidos y acordados en los planes de trabajo para la administración del servicio de aplicaciones que se presenten durante la vigencia del contrato.
- 7.1.177. 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.
- 7.1.178. Generar, implementar y documentar estándares para la instalación y administración de aplicaciones previa aprobación por parte del ICBF.
- 7.1.179. Entregar un documento semestralmente en medio físico y magnético. cuando lo requiera el ICBF, con recomendaciones sobre las aplicaciones para mejorar las condiciones de seguridad, disponibilidad y desempeño de la infraestructura que soporta las aplicaciones.
- 7.1.180. Realizar diagnósticos y análisis de seguimiento de forma permanente a las aplicaciones del ICBF y hacer la entrega de los resultados mediante un informe.
- 7.1.181. Hacer seguimiento y documentar controles de cambios, controles de accesos, y actualización a las aplicaciones.
- 7.1.182. Mantener actualizado el inventario de Aplicaciones de acuerdo al formato establecido entre EL CONTRATISTA y el ICBF. Además generar mapas de servidores de aplicaciones, bases de datos, conexiones lógicas y físicas y actualización mensual de los mismos.

- 7.1.183. Realizar análisis detallado de incidentes, gestión de problemas y actividades tales como análisis de tendencias, análisis de causa raíz y establecimiento de error conocido, información que se debe registrar en un documento.
- 7.1.184. 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.
- 7.1.185. 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.
- 7.1.186. Proponer plan de trabajo en donde se contemplen acciones de mejora y mantenimiento de las aplicaciones del ICBF
- 7.1.187. Informar los riesgos de operatividad, seguridad y degradación del servicio identificando puntos críticos y definiendo e implementando acciones previa autorización del ICBF.
- 7.1.188. 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.
- 7.1.189. Atender las solicitudes y requerimientos respectivos al servicio de aplicaciones de la entidad (cambios, comunicación, configuración, despliegue, monitoreo) de acuerdo a los tiempos que establezca el ICBF.
- 7.1.190. Apoyar técnicamente al ICBF en el diseño, implementación, medición y administración de pruebas piloto relacionadas con este servicio.
- 7.1.191. Diseñar, elaborar, socializar y ejecutar el plan de mantenimiento anual para el servicio de administración de aplicaciones.
- 7.1.192. Recopilar y guardar la información estadística de aplicaciones como soporte para el cálculo de los indicadores, esta información puede ser solicitada por la ICBF en cualquier momento.

- 7.1.193. En caso que sea requerido EL CONTRATISTA deberá diseñar, implementar y administrar soluciones de virtualización de aplicaciones a través del hardware y software suministrado por el ICBF.

## Base de datos

### Servicios de Administración y operación

- 7.1.194. EL CONTRATISTA es el responsable de la 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.
- 7.1.195. Desarrollar, documentar e implementar planes de mantenimiento de Bases de Datos. Las tareas de mantenimiento se podrán verificar a través de los archivos de log de ejecución y serán enviadas según solicitud del ICBF.
- 7.1.196. 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.
- 7.1.197. Llevar el control de las licencias del motor de base de datos SQL Server adquiridas versus las utilizadas e informar oportunamente al ICBF.
- 7.1.198. Realizar un Informe mensual sobre el comportamiento de las bases de datos que incluya como mínimo: informe de bloqueos (deadlock), recomendaciones, comportamiento estadístico de índices, recomendaciones para particionar tablas, vistas, top 10 de sentencias que consuman más recursos.
- 7.1.199. 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.
- 7.1.200. EL CONTRATISTA es responsable de realizar los traslados físicos de las bases de datos, bajo solicitud y aprobación del ICBF, mediante un proceso de control de cambios, previa aprobación del comité de control de cambios.
- 7.1.201. Definir, documentar y comunicar las políticas, procedimientos y estándares de conexión de las bases de datos antes de ser publicados y una vez aprobados por el ICBF.

- 7.1.202. Documentar las causas y acciones a tomar en aquellas bases de datos que estén por debajo del 100% en disponibilidad, esto debe ser un anexo al informe mensual de gestión.
- 7.1.203. 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.
- 7.1.204. Generar y presentar un cronograma de las actividades de mantenimiento de las bases de datos con fechas de ejecución y responsables, el cual debe ser validado por el ICBF.
- 7.1.205. Brindar apoyo técnico 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.
- 7.1.206. Designar personal especializado de acuerdo al Anexo 006 - PERFILES PROFESIONALES REQUERIDOS que se encuentre disponible de forma permanente (7X24X365) para responder a las alertas y/o incidentes generados en la plataforma tecnológica, y que afecte el servicio de base de datos.
- 7.1.207. Notificar al ICBF cualquier incidente que afecte la prestación del servicio, a través de correo electrónico y/o telefónicamente o por otro medio disponible y actuar proactivamente en la búsqueda y aplicación de la solución.
- 7.1.208. Diseñar, crear, documentar y mantener actualizados los procesos, procedimientos, lineamientos e instructivos del servicio de base de datos en común acuerdo con EL ICBF.
- 7.1.209. 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 en los tiempos definidos por El ICBF.
- 7.1.210. Apoyar técnicamente a la Subdirección de Recursos Tecnológicos en la generación de conocimiento relacionado con el servicio, para su uso y registro en la base de datos de conocimientos de TI del ICBF.
- 7.1.211. 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.

## **Correo Electrónico**

### **Servicios de Administración y operación**

- 7.1.212. 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.
- 7.1.213. Informar quincenalmente 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,
- 7.1.214. Gestionar y documentar los incidentes en la herramienta definida por el ICBF con la información pertinente, en los tiempos establecidos.
- 7.1.215. Notificar al ICBF (líder del servicio) cualquier incidente que afecte la prestación del servicio 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.
- 7.1.216. 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.

## **Herramientas De Gestion, Monitoreo Y Seguridad**

### **Centro de Monitoreo y Gestión**

- 7.1.217. 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.

- 7.1.218. Monitorear los servicios en tiempo real por medio de herramientas automatizadas propias del ICBF y/o CONTRATISTA que envíen notificaciones a la herramienta de Mesa de servicio de acuerdo a su nivel de criticidad y cuya información permita generar acciones proactivas.
- 7.1.219. Monitorear 7X24X365 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.
- 7.1.220. 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.
- 7.1.221. Configurar las acciones automáticas ante caídas del servicio, mediante envío de popup, e-mail, mensajes de consola, etc. El personal designado por el ICBF deberá recibir mensajes de notificación a los teléfonos móviles (Mensajería Instantánea, Email), cuando se presenten caídas de los Servicios.
- 7.1.222. Monitorear el uso de recursos lógicos de los dispositivos a través de los agentes activos instalados para tal efecto.
- 7.1.223. Identificar en forma temprana posibles fallas en los sistemas y dispositivos de los servicios.
- 7.1.224. Actuar de inmediato ante la aparición de incidentes o alarmas para buscar su solución. El CMG (Centro de Monitoreo y Gestión) constituye un primer nivel de atención y deberá generar un caso para atención de segundo nivel.
- 7.1.225. 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.
- 7.1.226. Ejecutar y registrar la gestión realizada en la herramienta de Mesa de Servicio, 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.
- 7.1.227. Completar la categorización o re-categorizar los incidentes asignados ya sea por Mesa de Servicio o por la Herramienta de gestión en caso de ser necesario.

- 7.1.228. Aplicar los parches de mantenimiento de software preventivo y correctivo (parches, fixes o service packs) del software de monitoreo para corregir defectos.
- 7.1.229. Definir y mantener actualizada, en asocio con ICBF, la lista de contactos para el escalamiento del servicio de monitoreo.
- 7.1.230. 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.

### **Herramientas de Monitoreo, Gestión y Seguridad**

- 7.1.231. Garantizar la gestión y el monitoreo de la Infraestructura desde el primer día de la operación mediante la herramienta propiedad del ICBF.  
Nota: El contratista podrá usar herramientas adicionales en los casos que SystemCenter no cumpla con requisitos de administración, monitoreo y gestión del presente capítulo.
- 7.1.232. Implementar y operar los todos módulos System Center que estén disponibles en el ICBF para el monitoreo y control de la infraestructura el ICBF. El ICBF podrá solicitar la implementación y/o modificación, técnica, funcional y operativa de cualquiera de los módulos de la suite System Center. 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.
- 7.1.233. 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.
- 7.1.234. El contratista deberá garantizar el debido funcionamiento de WSUS integrado con SystemCenter durante toda la ejecución del contrato.
- 7.1.235. Presentar informe mensual de herramientas de gestión y monitoreo donde se incluya el estado y gestión de las mismas.

- 7.1.236. Realizar y/o Actualizar toda la documentación que el ICBF requiera respecto al servicio de Herramientas de Gestión y Monitoreo, la documentación debe estar alojada en los repositorios que el ICBF designe para tal fin.
- 7.1.237. 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 en pro del beneficio y utilización de herramientas propias del ICBF.
- 7.1.238. Implementar, mejorar, optimizar o actualizar los servicios de los distintos módulos de SystemCenter con el fin de realizar la gestión de Administración, Gestión y Monitoreo acordes a las necesidades del ICBF y su infraestructura tecnológica.
- 7.1.239. Utilizar System Center para resolver cualquiera de los requerimientos del presente anexo técnico, siempre y cuando la herramienta lo realice de forma nativa o con los módulos certificados por fabricante para este fin (Configurations y Management Packs), en caso de que el módulo 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 módulo debe realizar las integraciones pertinentes con otros servicios y/o contratos dentro del marco del presente anexo técnico, toda implementación y/o acción debe quedar debidamente documentada.
- 7.1.240. En caso de que la Suite System Center o las herramientas antes expuestas no cumplan algún requerimiento del presente capítulo, 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.
- 7.1.241. 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.
- 7.1.242. Las herramientas utilizadas por parte del CONTRATISTA deben ser de dedicación exclusiva del ICBF durante la ejecución del Contrato.
- 7.1.243. Mantener, Administrar y Operar las herramientas de gestión que están actualmente implementadas en el ICBF.

- 7.1.244. Suministrar Herramienta(s) en caso de que las herramientas del ICBF de forma comprobada técnicamente no cumplan algún requerimiento que se solicite.
- 7.1.245. Implementar y configurar los dashboard que el ICBF solicite durante la ejecución del CONTRATO en el marco de los servicios con que cuenta la entidad.
- 7.1.246. Permitir la generación de notificaciones de eventos y alarmas en tiempo real para la creación automática de tickets para la herramienta de gestión de mesa de servicio del ICBF y que éstas también lleguen al personal designado por el ICBF.
- 7.1.247. Programar y realizar capacitaciones y transferencia de conocimiento con una duración mínima de 120 horas en lo que concierne a la operación, dirigidas al menos para 60 personas designadas por el ICBF, donde se incluya: herramientas de gestión, monitoreo y diagnóstico provistas por EL CONTRATISTA y las demás herramientas que se utilicen durante el desarrollo del proyecto. Las capacitaciones deben realizarse de manera periódica cuando existan actualizaciones sobre las herramientas o cambios en el personal designado por el ICBF.
- 7.1.248. Gestionar la administración y monitoreo de todos los Ítems solicitados en el capítulo de HERRAMIENTAS DE GESTION Y MONITOREO del presente documento, a través de las herramientas propias del ICBF y/o suministradas por El Contratista en caso de ser necesario, permitiendo generar esquemas de monitoreo personalizables y accesibles.

### **Administración y Monitoreo de Puntos Finales**

- 7.1.249. 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.
- 7.1.250. Gestionar el adecuado descubrimiento automático de hardware y software de todos los Endpoints 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.

- 7.1.251. Administrar y Gestionar a nivel lógico todos los end points que puedan estar conectados al Directorio Activo y/o a la red del ICBF, o que sean suministrados por el mismo, y se registrarán bajo los lineamientos que el ICBF disponga para este fin.
- 7.1.252. Realizar despliegue de Aplicaciones, Configuraciones, Scripts, Componentes de Software a través de SystemCenter según lo requiera el ICBF.
- 7.1.253. Activar, administrar, gestionar, monitorear y soportar el licenciamiento de todos los end points del ICBF usando las herramientas entregadas por ICBF (System Center, Servidor KMS para Licenciamiento Microsoft, servidor de licencias autocad, servidor de licencias SPSS, otros) y suministrar las demás herramientas necesarias para administrar el licenciamiento que se adquiera o que no esté cubierto por las herramientas entregadas por ICBF.
- 7.1.254. Mantener control de la línea base de Licenciamiento y el número de máquinas reportadas por las herramientas (máquinas activas y de laboratorio), para así trabajar en conjunto con el ICBF en la correcta gestión y control del licenciamiento que el ICBF tiene adquirido.
- 7.1.255. 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

## **Redes de Área Local (LAN)**

### **Servicios de Administración y operación**

- 7.1.256. Administrar, operar y monitorear los equipos activos de la red LAN de las sedes de la Dirección General y Sedes Anexas.
- 7.1.257. Mantener actualizados los inventarios de la infraestructura de la red LAN en las sedes de la Dirección General y Sedes Anexas en el formato que el ICBF designe.
- 7.1.258. Desarrollar actividades periódicas de análisis de tráfico en redes LAN. Dichas actividades se desarrollarán trimestralmente y como resultado de ellas, EL CONTRATISTA presentará un informe detallando el análisis de protocolos realizado, porcentaje de utilización de ancho de banda por protocolo, hallazgos de seguridad y hallazgos relacionados con configuraciones de switching en las redes y sus

respectivos planes de acción para corregir problemas y mejorar las condiciones o configuraciones actuales.

- 7.1.259. Mantener actualizada la documentación de la topología de las redes LAN de las sedes de la Dirección General y Sedes Anexas, incluyendo diagramas y planos, en medio magnético y notificar los cambios vía correo electrónico a la persona encargada en el ICBF.
- 7.1.260. Realizar el escalamiento de incidentes al proveedor de MESA DE SERVICIO los problemas de hardware o software que deba escalarse al fabricante de los equipos de red administrados.

### **Redes Inalámbricas (WLAN)**

#### **Servicios de Administración y operación**

- 7.1.261. El Contratista debe realizar la administración, configuración, monitoreo y soporte de la RED INALAMBRICA (WLAN) para la sede de la Dirección General de la Entidad y la Sede de la dirección de Información y Tecnología.
- 7.1.262. Entregar un informe de zonas de cobertura bimensual como mínimo, o cuando el ICBF lo requiera.
- 7.1.263. Llevar control y actualización del inventario de Access Points de acuerdo al formato establecido por el ICBF.
- 7.1.264. Configurar y dar soporte al portal cautivo para ingreso de visitantes a la red WLAN del ICBF de acuerdo a las políticas establecidas por el ICBF.
- 7.1.265. Realizar el escalamiento de incidentes al proveedor de MESA DE SERVICIO los problemas de hardware o software que deba escalarse al fabricante.

### **Gobernabilidad**

Suministrar 14 Smartphones de acuerdo con lo indicado en el numeral Elementos de Comunicación la introducción del Anexo Técnico.

---

## **Internet Móvil**

- 7.1.1. El Contratista deberá prestar el servicios de internet móvil dentro de los 15 días calendario siguientes a la firma del contrato, para ello debe suministrar 250 dispositivo con conexión inalámbrica a internet móvil público por puerto USB, con sus respectivas tarjetas SIM con velocidad 4G LTE/3.5G con servicio de Internet limitado con 3 Gigabytes de datos o con 4 Gigabyte, y 40 dispositivos MIFI con sus respectivas tarjetas SIM con velocidad 4G LTE con servicio de Internet limitado con 8 Gigabyte de datos o con 10 Gigabyte.
- 7.1.2. El Contratista deberá activar los módems máximo 48 horas siguientes a la realización de la solicitud de activación por parte del ICBF. La prestación del servicio de internet móvil, y por ende su cobro, comenzará a contar a partir de la fecha de activación de los módem por parte del Contratista, previa solicitud del ICBF.
- 7.1.3. Entregar un Informe Inicial de cobertura Nacional del proveedor o proveedores de Internet Móvil.
- 7.1.4. Entregar reportes de consumo mensualmente sobre el estado de cada uno de los módems suministrados por El Contratista.
- 7.1.5. El Contratista deberá reemplazar los módems USB con equipos MIFI en la medida en que la tecnología MIFI con velocidades 4G LTE tenga cobertura en las regiones de distribución de los equipos que designe el ICBF.

## **Relacionadas con planes**

- 7.1.6. Desarrollar los planes para la gerencia del proyecto relacionados en el numeral 6.6.13.4
- 7.1.7. 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.
- 7.1.8. 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.

## **Relacionadas con equipo de trabajo**

- 7.1.9. Proveer el personal requerido de acuerdo a los roles establecidos en el capítulo de Gobernabilidad y el ANEXO 006 ANEXOS PROFESIONALES REQUERIDOS. El personal debe ser de dedicación exclusiva para el desarrollo del contrato.
- 7.1.10. Prestar los servicios con personal calificado y especializado que cumpla con los perfiles y experiencia exigidos por el ICBF como se indica en el Anexo 006 - PERFILES-PROFESIONALES REQUERIDOS.
- 7.1.11. El Contratista debe garantizar la operación de los servicios 7X24X365 durante la ejecución del contrato con el personal mínimo relacionado en el Anexo 006 - PERFILES-PROFESIONALES REQUERIDOS, y el personal analista y de apoyo capacitado y calificado para la prestación de los servicios.
- 7.1.12. Para el caso de renunciaciones, 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.
- 7.1.13. Presentar quincenalmente el cronograma de disponibilidad del personal de EL CONTRATISTA asignado al proyecto.
- 7.1.14. Presentar notificación con 8 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.
- 7.1.15. Diseñar, entregar y aplicar los formatos, procesos y procedimientos para la prestación del servicio con el detalle que el ICBF lo exija.
- 7.1.16. Designar personal especializado que se encuentre disponible de forma permanente (7X24X365) para responder a las alertas y/o incidentes generados en la plataforma tecnológica.
- 7.1.17. Disponer de un especialista por servicio, el cual estará en constante comunicación con el líder del respectivo servicio designado por el ICBF.
- 7.1.18. Garantizar que la incorporación y/o sustitución de alguno de los especialistas, sea informado con 8 días de antelación al ICBF y este debe cumplir con el Anexo 006 - PERFILES-PROFESIONALES REQUERIDOS.
- 7.1.19. 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.

7.1.20. Informar al ICBF los compensatorios de los especialistas quincenalmente.

7.1.21. 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.

#### **Relacionadas con comités**

7.1.22. 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, de acuerdo a lo descrito en el numeral 6.6.15.3 del Anexo Técnico.

#### **Relacionadas con documentación e informes**

7.1.23. Elaborar y mantener actualizada en últimas versiones en medio físico y digital toda la documentación relacionada con el presente contrato incluyendo: actas, informes, planes de gestión, planes de mejoramiento y las demás relacionadas con el objeto del contrato.

7.1.24. Realizar, administrar y mantener actualizado un repositorio de información en donde se almacene la información generada o resultante del presente contrato en donde se administre las versiones de los documentos.

7.1.25. 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.

7.1.26. Presentar informes mensuales de gestión (por servicio) que reflejen el desempeño en la ejecución de los servicios, y el informe de los ANS. Los informes mensuales debe contener 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 (Informes mensuales de gestión y de ANS) deben entregarse a cada uno de los líderes de los servicios del ICBF en los primeros 5 días hábiles del mes. En caso de ser necesario realizar correcciones a dichos informes el Contratista contará con máximo 3 días hábiles adicionales para realizar dichas correcciones una vez se realice la devolución de los informes. En todo caso la entrega de los informes no puede superar los primeros 10 días hábiles del

mes. La no presentación a tiempo de los informes mensuales generará penalizaciones según el Anexo 002 - ACUERDOS DE NIVELES DE SERVICIO.

- 7.1.27. El Contratista deberá presentar la factura de los servicios efectivamente prestados dentro de los primeros 10 días hábiles de cada mes. Igualmente debe presentar como soporte a dicha factura los informes de mensuales de gestión (por servicio del respectivo periodo facturado) y el informe de ANS aprobados por el ICBF. La no presentación a tiempo de la factura generará penalizaciones según el Anexo 002 - ACUERDOS DE NIVELES DE SERVICIO.
- 7.1.28. Documentar detalladamente los procedimientos, instructivos e instrumentos técnicos a utilizar durante los cambios que se requieran sobre cualquiera de los 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.
- 7.1.29. 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.
- 7.1.30. 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.
- 7.1.31. Guardar debida y completa reserva y confidencialidad sobre la información y los documentos del ICBF que tenga conocimiento o a los que tenga acceso en virtud del objeto del contrato.
- 7.1.32. 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.
- 7.1.33. 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.

7.1.34. 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.

7.1.35. El detalle de los informes generados y requeridos en cada uno de los servicios deben ser previamente pactado entre el ICBF y el Contratista, adicionalmente debe entregarse en los medios en que el ICBF los requiera (físicos, Magnético, correo).

#### **Relacionadas con el inventario**

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

#### **Relacionadas con herramientas**

7.1.37. Gestionar en la herramienta de gestión de mesa de servicio que disponga el ICBF los tickets asignados referentes a incidentes, requerimientos y controles de cambios de los diferentes servicios a cargo del Contratista. Esta gestión de tickets consiste en la consulta, documentación de trámite y solución y cierre de los mismos.

7.1.38. 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.

7.1.39. 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.

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

---

### Relacionadas con el inventario

7.1.41. Mantener actualizado el inventario de la infraestructura administrada incluyendo la topología de los mismos, la cual deberá ser reportada al ICBF.

### Relacionadas con los servicios

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

7.1.43. Garantizar la operación en los servicios bajo los horarios, tiempos de respuesta y condiciones establecidas en el presente Anexo Técnico y Anexo 002 ACUEROS DE NIVELES DE SERVICIO.

7.1.44. 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.

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

7.1.46. Licenciar todo el software que provea y disponga para dar cumplimiento al objeto del contrato.

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

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

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

7.1.50. Desarrollar un plan de capacidad para todos los servicios objeto del presente contrato como mínimo una vez al año, donde se evalúe el planteamiento de la suficiencia de la infraestructura del ICBF, así como la proyección y pertinencia de realizar nuevas adquisiciones o mejoras.

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

#### **Relacionadas con seguridad**

7.1.52. 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 en lo pertinente a infraestructura tecnológica.

7.1.53. 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).

7.1.54. 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.

7.1.55. Mantener monitoreados los servicios 7X24X365, durante la duración del contrato.

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

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

7.1.58. 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.

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

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

#### **Relacionadas con calidad**

7.1.61. Trabajar, en conjunto con la SRT en la gestión para el tratamiento y cierre de acciones preventivas, correctivas o de mejora, relacionada con los servicios objetivo del

presente contrato 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.

- 7.1.62. Llevar el registro de los controles de cambios para las actividades que afecten los ambientes administrados.
- 7.1.63. 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.
- 7.1.64. 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.
- 7.1.65. Acoger las recomendaciones que durante la vigencia del contrato realice la SRT, las cuales contribuyan en la mejora de prestación del servicio.
- 7.1.66. Generar y ejecutar de forma anual el cronograma de las actividades de mantenimiento con fechas y responsables para la infraestructura y los servicios.
- 7.1.67. Brindar apoyo técnico 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.
- 7.1.68. Garantizar al ICBF la confidencialidad y accesos a la información, para esto se compromete a firmar y cumplir el acuerdo de confidencialidad.
- 7.1.69. 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.
- 7.1.70. 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.

7.1.71. Realizar la gestión con terceros de incidentes y requerimientos que así lo requieran, previa autorización del ICBF.

## **7.2 Obligaciones Generales del Contratista:**

- 7.2.1 Asumir la responsabilidad de todas las actividades relativas a la ejecución de las obligaciones establecidas en este contrato.
- 7.2.2 Participar y apoyar a EL ICBF en todas las reuniones a las que éste lo convoque relacionadas con la ejecución del contrato.
- 7.2.3 Disponer de los medios necesarios para el mantenimiento, cuidado y custodia de la documentación objeto del presente contrato.
- 7.2.4 Devolver a la Dirección administrativa del ICBF los documentos y archivos que en desarrollo del contrato se le hayan entregado, y a la misma los bienes devolutivos que le fueron asignados para su custodia.
- 7.2.5 Colaborar con EL ICBF en el suministro y respuesta de la información correspondiente a los requerimientos que realicen los órganos de control.
- 7.2.6 Utilizar la imagen del ICBF de acuerdo con los lineamientos establecidos por éste. Salvo autorización expresa y escrita de las partes ningún funcionario, podrá utilizar el nombre, emblema o sello oficial de la otra parte para fines publicitarios o de cualquier otra índole.
- 7.2.7 Realizar los pagos al SGSS (salud, pensión y riesgos profesionales), de acuerdo con la normatividad vigente aportando los soportes de pago correspondientes.
- 7.2.8 Constituir y allegar a EL ICBF las garantías requeridas dentro de los tres (3) días hábiles siguientes a la suscripción del convenio.

## **7.3. Obligaciones del Sistema Integrado de Gestión:**

### **7.3.1. Para el eje de Calidad**

- 7.3.1.1. El 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 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**

- 7.3.2.1. El 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 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 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.

## **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 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 32 meses, contados a partir de la legalización del contrato hasta el 31 de julio de 2018.

En los primeros 15 días, EL CONTRATISTA debe recibir del actual operador y de ICBF los servicios tecnológicos a operar y realizar las instalaciones iniciales indispensables de la infraestructura y recursos que requiera. En los siguientes 31,5 meses, EL CONTRATISTA realizará la operación y administración de los servicios contratados, garantizando la continuidad en la prestación de los mismos y de la plataforma tecnológica. En los últimos 2 meses del contrato, EL CONTRATISTA deberá realizar empalme y entrega del servicio al nuevo operador.

## **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 y 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.

### **Forma de pago:**

El ICBF realizara pagos mensuales al CONTRATISTA por los servicios efectivamente prestados y aplicados los descuentos correspondientes.

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

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

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

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

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. TIPIFICACIÓN, ESTIMACIÓN Y ASIGNACIÓN DE LOS RIESGOS PREVISIBLES**

Con el fin de conocer los riesgos que afectarían el contrato que se pretende adelantar, tanto en aspectos favorables como adversos; y con el fin de contribuir a asegurar los fines que el estado persigue con la contratación, el ICBF ha preparado este anexo, el cual permite dilucidar aspectos que deben ser considerados en la adecuada estructuración de ofertas y planes de contingencia y continuidad del proyecto.

De este modo, corresponderá al contratista seleccionado la asunción del riesgo previsible propio de este tipo de contratación, asumiendo su costo, siempre que el mismo no se encuentre expresamente a cargo del ICBF en el Pliego de Condiciones.

Los riesgos que podrían afectar el normal desarrollo de las actividades previstas en esta contratación son:

| No | Clase   | Fuente  | Etapas     | Tipo                  | Descripción (Qué puede pasar y, cómo puede ocurrir)                                                                          | Consecuencia de la ocurrencia del evento                               | Probabilidad | Impacto  | Valoración del riesgo | Categoría   | ¿A quién se le asigna?        | Tratamiento/Controles a ser implementados | Impacto después del tratamiento |                |                       |             | ¿Afecta la ejecución del contrato? | Persona responsable por implementar el tratamiento |
|----|---------|---------|------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|--------------|----------|-----------------------|-------------|-------------------------------|-------------------------------------------|---------------------------------|----------------|-----------------------|-------------|------------------------------------|----------------------------------------------------|
|    |         |         |            |                       |                                                                                                                              |                                                                        |              |          |                       |             |                               |                                           | Probabilidad                    | Impacto        | Valoración del riesgo | Categoría   |                                    |                                                    |
| 1  | General | Externo | Planeación | Riesgos Operacionales | Que no se presenten proponentes a la licitación                                                                              | Declara como desierta la contratación                                  | Raro         | Moderado | 4                     | Riesgo Bajo | Área de contratación del ICBF | Aceptar el Riesgo                         | Raro                            | Insignificante | 2                     | Riesgo Bajo | SI                                 | Área de contratación del ICBF                      |
| 2  | General | Externo | Ejecución  | Riesgos Financieros   | Volatilidad de las tasas de cambio                                                                                           | Aumento en los precios de los elementos con lo que prestan el servicio | Probable     | Moderado | 7                     | Riesgo Alto | Proveedor                     | Reducir la probabilidad                   | Raro                            | Menor          | 3                     | Riesgo Bajo | SI                                 | Proveedor                                          |
| 3  | General | Externo | Ejecución  | Riesgos Operacionales | Retraso en la importación de los elementos, partes y/o repuestos requeridos por el ICBF para la prestación de los servicios. | Sanción económica al proveedor de acuerdo a lo pactado en los ANS      | Raro         | Menor    | 3                     | Riesgo Bajo | Proveedor                     | Reducir la probabilidad                   | Raro                            | Insignificante | 2                     | Riesgo Bajo | SI                                 | Proveedor                                          |

| No | Clase   | Fuente  | Etapas    | Tipo                  | Descripción (Qué puede pasar y, cómo puede ocurrir)                                                                                         | Consecuencia de la ocurrencia del evento            | Probabilidad | Impacto | Valoración del riesgo | Categoría    | ¿A quién se le asigna? | Tratamiento/Controles a ser implementados | Impacto después del tratamiento |                |   |             | ¿Afecta la ejecución del contrato? | Persona responsable por implementar el tratamiento |
|----|---------|---------|-----------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|--------------|---------|-----------------------|--------------|------------------------|-------------------------------------------|---------------------------------|----------------|---|-------------|------------------------------------|----------------------------------------------------|
| 4  | General | Externo | Ejecución | Riesgos Operacionales | Incumplimiento por parte de terceros en la entrega y/o aprovisionamiento de los dispositivos necesarios para la prestación de los servicios | Incumplimiento en la entrega del objeto contractual | Posible      | Menor   | 5                     | Riesgo Medio | Proveedor              | Reducir la probabilidad                   | Posible                         | Insignificante | 4 | Riesgo Bajo | Si                                 | Proveedor                                          |

## 12. ANEXOS

- ANEXO 001-LINEA BASE-INFRAESTRUCTURA.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 - EQUIPOS - RED LAN -WLAN.xlsx
- Anexo 009 - INVENTARIO EQUIPOS DATACENTER EXTERNO.xlsx
- Anexo 010 - BACKUPS.xlsx
- Anexo 011 - EQUIPOS DE TELEFONÍA IP POR SEDE.xlsx
- Anexo 012 - SERVIDORES EN CLOUD
- Anexo 013 - INVENTARIO DE APLICACIONES
- Anexo 014 - INVENTARIO DE CERTIFICADOS DIGITALES

## 13. ACEPTACIÓN CUMPLIMIENTO DE REQUERIMIENTOS TÉCNICOS

Señor proveedor o contratista potencial: Al remitir cotización y/o propuesta, usted está aceptando que la misma cumple con la totalidad de los requerimientos incluidos en el presente documento y que incluye la totalidad de costos y gastos, directos e indirectos, así como los impuestos,

asociados a la ejecución del contrato. Así mismo, que en caso de resultar adjudicatario del proceso de selección correspondiente, podrá prestar el servicio y/o entregar el bien, con las condiciones técnicas descritas en el presente documento.

|                                              |                                                                 |                                                                     |
|----------------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------|
|                                              |                                                                 |                                                                     |
| Elaboró                                      | Revisó                                                          | Aprobó                                                              |
| Luis Armando Solarte<br>Gerente de Proyectos | Héctor Germán Páramo<br>Subdirector de Recursos<br>Tecnológicos | Piedad Cecilia Montero<br>Directora de Información y<br>Tecnología. |