| F02 - ANEXO – CONDICIONES TÉCNICAS ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DE BIEN | Fecha | 16/09/13 |
|---|---|---|

## 1. DENOMINACIÓN DEL BIEN O SERVICIO

Contratar el servicio especializado de consultoría que incluya realizar el diagnóstico de seguridad, análisis de riesgos, BCP, BIA, DRP, Red Segura, Nomograma y sensibilización al personal de ICBF y la elaboración del Plan estratégico de seguridad de la Información, De acuerdo al Modelo de seguridad de tecnología de información y comunicaciones para el ICBF, con el fin de dar continuidad de la certificación ISO 27001, la aplicación de esta consultoría se realizará en la obertura descrita en el Anexo 1 listado de regionales y/o centros zonales. del presente documento.

## 2. DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO

N/A

## 3. UNIDAD DE MEDIDA

N/A

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

Norma ISO 27001 – Sistema de Gestión de la Seguridad de la Información

## 5. DESCRIPCIÓN GENERAL

De acuerdo al Modelo de seguridad de tecnología de información y comunicaciones para el ICBF, con el fin de cubrir las necesidades definidas en su primera fase y dar continuidad de la certificación ISO 27001 se requiere contratar una consultoría en la cual se incluyan los siguientes aspectos:

- Diagnóstico de Seguridad Física y Lógica de la Entidad.
- Análisis de Riesgos.
- BCP (Plan de Continuidad del negocio o sus siglas en inglés, Business Continuity Plan**)**
- BIA (Análisis de Impacto del Negocio en inglés Business Impact Analysis)
- DRP (Plan de Recuperación Ante Desastres en Inglés Disaster Recovery Plan)
- Red Segura.
- Normograma.
- Sensibilización al personal de ICBF.
- Plan Estratégico Seguridad de la Información: Identificar el conjunto de responsabilidades, prácticas y acciones a ser desarrolladas por la organización con miras a propender que los riesgos de la información sean apropiadamente



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

administrados, mediante la definición de un modelo de seguridad de la información, alineado con las mejores prácticas, estándares y objetivos del negocio.

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

### 6.1. CONSULTORÍA PARA LA CONTINUIDAD DE LA CERTIFICACIÓN ISO 27001 QUE INCLUYA REALIZAR DIAGNÓSTICO DE SEGURIDAD, EL ANALISIS DE RIESGOS, BCP, BIA, DRP, RED SEGURA Y SENSIBILIZACIÓN AL PERSONAL DE ICBF

La consultoría se debe desarrollar en las Regionales y Centros Zonales mínimos que se relacionan en el Anexo No. 1. “listado de regionales y/o centros zonales”, las cuales podrán cambiar durante el desarrollo de la consultoría, los costos de traslados a dichos lugares deben ser asumidos por el contratista.

Para el desarrollo de la consultoría el ICBF hace entrega del Anexo No. 2 “Fases de ejecución” con los tiempos establecidos para el cumplimiento de los ítems que se describen a continuación:

#### 6.1.1 Diagnóstico De Seguridad.

Basado en la norma ISO/IEC27002:2005 y en los lineamientos de sus 11 dominios, el Contratista debe desarrollar un levantamiento de Información que permita evaluar y diagnosticar el nivel de cumplimiento del ICBF respecto a cada uno de ellos en las ubicaciones descritas en el Anexo No. 2 fases de ejecución, entregado por el ICBF. En esta etapa se debe:

- El contratista debe presentar un documento formal al ICBF del plan de Levantamiento de Información para la respectiva para aprobación.
- El contratista debe efectuar un diagnóstico de la situación en materia de seguridad informática, revisando y analizando el esquema actual respecto a todo lo establecido en la familia de estándares ISO27001-2005, y presentar la línea base de seguridad que indique donde se encuentra la Entidad respecto a los mismos, generando en el análisis de brecha las acciones a realizar para cumplir lo indicado en estos.
- El contratista debe recopilar las políticas, normas, lineamientos, procedimientos instructivos, formatos, manuales, tablas de retención, planes de contingencia existentes y demás recursos con los que cuenta el ICBF, evaluar su efectividad. El levantamiento de esta información se realizará con el acompañamiento del ICBF.
- El contratista debe verificar el estado de los dominios y controles mencionados en la norma ISO/IEC 27001.
- El contratista debe presentar al ICBF las evidencias, hallazgos, conclusiones, observaciones y recomendaciones como resultado del análisis de brecha.
- Toda la información resultante de esta fase de diagnóstico debe entregarse en medio magnético y físico al ICBF.



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

### 6.1.2 Análisis de Riesgos.

El desarrollo de esta actividad permitirá identificar, analizar, evaluar y definir las actividades para el tratamiento de los riesgos de seguridad de la información en el ICBF, para así apoyar el cumplimiento de los objetivos estratégicos de la entidad, el tratamiento debe estar encaminado a disminuir a un nivel aceptable el impacto de la materialización de dichos riesgos, el desarrollo de esta etapa se debe ejecutar de acuerdo al Anexo No. 2 fases de ejecución, adicional debe tenerse en cuenta:
El contratista debe verificar y proponer mejoras a la metodología de análisis de Riesgos que pertenece al ICBF de acuerdo a los estándares reconocidos.

- El contratista debe definir los criterios de probabilidad, impacto, riesgo, niveles aceptables y postura (tolerancia, tratamiento, transferencia, eliminación) mediante los cuales se evaluarán y gestionarán los riesgos.
- La metodología que va a utilizar el contratista debe incluir al menos análisis de riesgos, evaluación de riesgos, tratamiento, revisión, monitoreo y comunicación. La metodología debe someterse a aprobación por parte del ICBF.
- El contratista debe efectuar pruebas de penetración (pen test), interno y externo, a la infraestructura tecnológica de la Entidad, tendiente a identificar y explotar las vulnerabilidades de los componentes de la misma, recolectar las evidencias, categorizar, evaluar y priorizar las vulnerabilidades en las operaciones de negocio, así como formular y evaluar las medidas de control o remediación correspondientes a ser ejecutadas por la Entidad. Estas pruebas se deben aplicar a los controladores de dominio, IP internas donde se encuentren servidores de Bases de Datos y aplicaciones que la Entidad considera misionales y 40 IP Públicas, estas pruebas deben entregar reporte de vulnerabilidades y deben comprobar que estas pueden ser explotadas.
- El contratista debe elaborar el plan de tratamiento de Riesgos en el cual se identifiquen fácilmente los controles necesarios para tomar una acción sobre el riesgo entre las que se encuentran evitar, mitigar o transferir los riesgos identificados.
- El contratista debe identificar las amenazas que puedan explotar las vulnerabilidades identificadas.
- El contratista debe determinar el impacto cuantitativo y/o cualitativo según sea posible con respecto a la confidencialidad, integridad y disponibilidad.
- El contratista debe determinar el impacto general de materialización del riesgo.
- El contratista debe determinar el riesgo residual si se implementan el tratamiento propuesto a futuro.
- El contratista debe elaborar y presentar el informe completo del análisis de amenazas.
- El contratista debe elaborar y presentar el Informe completo del análisis de vulnerabilidades.
- El contratista debe elaborar y presentar la matriz de valoración riesgos de seguridad de la información priorizada, identificando los activos, las amenazas, las vulnerabilidades, impactos, los riesgos y las acciones a realizar.
- El contratista debe elaborar y presentar Informe de identificación de procedimientos y controles necesarios para tratar el riesgo.



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

- Toda la información resultante de esta fase de diagnóstico debe entregarse en medio magnético y físico al ICBF.

#### 6.1.3 BCP (Plan de Continuidad del negocio o sus siglas en inglés, Business Continuity Plan) – BIA (Análisis de Impacto del Negocio en inglés Business Impact Analysis) – DRP (Plan de Recuperación Ante Desastres en Inglés Disaster Recovery Plan)

Se debe diseñar un BCP que permita garantizar la disponibilidad y continuidad de los servicios prestados por el ICBF, la ejecución de esta fase debe desarrollarse de acuerdo al Anexo No. 2 fases de ejecución y debe contener como mínimo:

- Análisis de impacto.
- Realizar la identificación de controles
- Realizar la identificación de riesgos
- Elaborar el plan de contingencia.
- Diseñar y aplicar las pruebas requeridas al plan de contingencia.
- Proponer estrategias de recuperación.
- Realizar recomendaciones para la recuperación de la operación.

#### 6.1.4 Normograma en Seguridad para la Entidad.

El contratista debe realizar verificación y actualización del Normograma y la Matriz de Requisitos legales de todos los procesos de la Entidad respecto a las leyes aplicables para el Sistema de Gestión de Seguridad de Información.

Realizar el análisis de las leyes de seguridad de Información actuales y la aplicación que debe hacer la entidad para el cumplimento de cada una de ellas.

Para esto debe contar con Abogados que conozcan el tema y sobre todo énfasis en SGSI, el desarrollo de esta fase debe hacerse de acuerdo al Anexo No. 2 fases de ejecución.

#### 6.1.5 Plan Estratégico Seguridad De La Información

Para el desarrollo del Plan estratégico de la organización debe hacerse de acuerdo al Anexo No. 2 fases de ejecución y debe cumplir los siguientes requerimientos:

##### 6.1.5.1 Conocimiento del ICBF

El conocimiento de la organización es importante para la definición de la estrategia, entender hacia dónde va la organización en el mediano y corto plazo, cuales son las regulaciones pertinentes al negocio que desarrolla, identificar la posición de la organización frente a la seguridad de la información, el contexto en el cual desarrolla el negocio y muchos elementos más permiten identificar las necesidades y requerimientos que el negocio de la organización requiere.



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

Mediante entrevistas elaboradas por el contratista y aprobadas por el ICBF a personas claves dentro de la organización y la revisión de los planes estratégicos existentes; incluyendo el de TICs, junto con la cadena de valor y la estructura organizacional, con el fin que esta información permita contextualizar y conocer el funcionamiento y operación de la entidad, fundamental para la identificación de objetivos de SI. El Líder de Seguridad de la Información brindará acompañamiento al contratista para realizar las actividades, los Directores y Subdirectores de la Entidad o las personas que ellos designen serán las personas claves para el conocimiento de la misma.

#### 6.1.5.2 Diagnóstico seguridad de la información

Identificar el estado actual de la seguridad de la información en la organización usando como marco de referencia normas internacionales que permitan identificar las iniciativas en seguridad existentes y su nivel de madurez.

Obtener información general preliminar de la infraestructura TICs que apoya los procesos del negocio que permite indicar las mejores prácticas a implementar para llegar a un nivel de seguridad deseado. Esta actividad debe estar articulada con la fase 6.1.1 de este documento.

#### 6.1.5.3 Alineación de Objetivos.

El contratista debe alinear los objetivos de la seguridad de la información con los objetivos de negocio, permite que el plan estratégico aporte valor real a la organización, favoreciendo y fortaleciendo el cumplimiento de los objetivos de negocio. Estos se deben detallarse en el documento del plan estratégico de Seguridad de la Información.

#### 6.1.5.4 Modelo Seguridad de la información

El Modelo de seguridad de la información es el pilar importante del plan estratégico, a partir de este modelo surgen las iniciativas propias de seguridad de la información. Esta actividad busca identificar el Modelo de seguridad a desarrollar dentro del Plan estratégico, para lo cual el contratista debe utilizar como marco de referencia los siguientes estándares:

- Norma ISO/IEC 27001:2005
- Norma ISO/IEC 27002
- COBIT
- ISA 99 (SCADA)

Adicionalmente se deben identificar las actividades a seguir en cada uno de estos proyectos durante el Plan de Acción al primer año.



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

### 6.1.6 Sensibilización Colaboradores del ICBF

- El contratista debe generar una estrategia de sensibilización y cultura organizacional alineada a Seguridad de la Información de acuerdo al SGSI, y el BCP, esta estrategia debe estar proyectada a una implementación de 3 años.

- La estrategia de sensibilización el contratista debe incluir las actividades de Informar a los usuarios sobre sus responsabilidades para la protección de la información las cuales estarán documentadas en las políticas y procedimientos.

- La estrategia de sensibilización y cultura organizacional debe ser enfocada a todos los usuarios del ICBF.

- La estrategia debe difundir los requerimientos de seguridad que los colaboradores del ICBF necesitan para tomar conciencia y conocer su papel en la protección de la información de la entidad.

- La estrategia debe explicar las mejores prácticas y reglas de comportamiento que deben tener los usuarios para poder obtener un nivel adecuado de protección de la información personal y de la entidad

- La estrategia debe concientizar a los colaboradores en la importancia de la seguridad de la información en la organización y el rol que juega cada uno de ellos en la consolidación y estructuración de un plan de seguridad eficiente y acorde con las necesidades del ICBF.

- La estrategia debe brindar a los usuarios un nivel de educación y compromiso sobre los temas de seguridad de la información en la entidad, buscando como objetivo final enfocar al ICBF hacia una cultura de seguridad basada en su SGSI.

- El contratista debe entregar al ICBF como material de la campaña de sensibilización los siguientes elementos:

  - El contratista debe proveer el material que estipule en la estrategia, estos deben incluir la impresión de material POP y suvenires, teniendo en cuenta que la línea base son aproximadamente 11.000 usuarios.

  - La estrategia debe incluir Ofrecer como mínimo dos (2) conferencias cada una para un auditorio mínimo de doscientos (200) personas, acerca de temas de sensibilización. Para cada una de estas conferencias el contratista debe hacer entrega de los respectivos videos de la conferencia en medio físico, las conferencias se llevaran a cabo en las instalaciones del ICBF.

  - Ofrecer Curso y certificación a mínimo (3) colaboradores del ICBF en BCP.



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

- Adicional debe incluir como mínimo tres (3) ejercicios presenciales de Ingeniería social, uno en la Sede Dirección General y los dos restantes de las regionales del alcance. Estas pruebas deben tener un documento en el que se estipule la población objetivo, la planeación, objetivo, actividades a realizar, tiempos, análisis de resultados.

## 6.2. ENTREGABLES

- En el desarrollo de la consultoría en seguridad de la información se requieren los siguientes productos: Diagnóstico de seguridad de la información: Documento en el cual se describan los controles evaluados, resultados del diagnóstico de seguridad, análisis de brecha.
- Propuesta de modelo de seguridad de la información: Documento en el cual se encuentre la proyección del modelo de seguridad de la información, infraestructura tecnológica y seguridad física, de acuerdo a la Norma ISO 27001.
- Plan estratégico a 3 años: Plan con actividades estratégicas con proyección para los próximos respecto a la seguridad informática y de la información del ICBF, se deben identificar el conjunto de responsabilidades, prácticas y acciones a ser desarrolladas por la institucion con miras a propender que los riesgos de la información sean apropiadamente administrados, mediante la definición de un modelo de seguridad de la información, alineado con las mejores prácticas, estándares y objetivos del negocio
- Plan de Acción a un año: Plan con actividades estratégicas con proyección a un año respecto a la seguridad informática y de la información del ICBF.
- Análisis de Riesgos: Documento que describa la metodología utilizada en Análisis de Riesgos, documento de análisis de riesgos, plan de tratamiento de riesgos.
- BCP, DRP BIA: documento que detalle el plan de Recuperación de desastre, Priorización de procesos del ICBF, Análisis de Impacto, y actividades de implementación del BCP.
- Normograma actualizado
- Documento con estrategia de sensibilización para los colaboradores del ICBF.

## 6.3. PERSONAL MINIMO REQUERIDO

| PERFILES MÍNIMOS REQUERIDOS PARA LA PRESTACIÓN DEL SERVICIO | | | | |
|---|---|---|---|---|
| **Cargo** | **Cantidad** | **Formación profesional** | **Experiencia Profesional (Descripción de la experiencia y años)** | **Dedicación** |
| Consultor en seguridad ISO27001 | 2 | graduados como Ingenieros de Sistemas, Ingenieros Informáticos, Ingenieros electrónicos o Ingenieros industriales, con maestría o especialización en | experiencia de dos años como consultor en diseño o implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) basados en ISO 27001 | 100% |



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

| PERFILES MÍNIMOS REQUERIDOS PARA LA PRESTACIÓN DEL SERVICIO | | | | |
|---|---|---|---|---|
| **Cargo** | **Cantidad** | **Formación profesional** | **Experiencia Profesional (Descripción de la experiencia y años)** | **Dedicación** |
| | | Seguridad de la Información o seguridad informática, Certificación CEH | | |
| Gerente de Proyecto | 1 | Profesional en Economía, Administración de Empresas, Contaduría, Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica o Ingeniería Industrial, especializado en Gerencia de Proyectos | • Experiencia específica mínima de tres (3) años en gerencia de proyectos de tecnologías de la información o seguridad de la información. | 100% |
| Abogado | 1 | Profesional en Derecho. | • Experiencia mínima de 2 años en normatividad de Sistemas de Gestión. | 50% |
| Documentador | 1 | Profesional en Ingeniería de Sistemas, Electrónica, Industrial o Eléctrica o Administrador de Empresas o Economista. | • Experiencia profesional mínima de tres (3) años. | 100% |

## 7. OBLIGACIONES DEL CONTRATISTA

### 7.1. Obligaciones específicas

El contratista, bajo su responsabilidad y autonomía y en cumplimiento del objeto descrito, cumplirá con las siguientes obligaciones:

7.1.1. Cumplir con plena autonomía técnica y administrativa con las actividades descritas y las especificaciones técnicas definidas en el numeral 6 “ESPECIFICACIONES TÉCNICAS DE LOS INSUMOS, BIENES, PRODUCTOS, OBRAS O SERVICIOS A ENTREGAR” del presente documento.
7.1.2. Cumplir con el lugar de ejecución del contrato, según lo señalado en el presente documento.
7.1.3. Lleva a cabo la consultoría en seguridad de la información de acuerdo a lo establecido en el documento.
7.1.4. Realizar sensibilización de acuerdo con lo definido en el presente documento.



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

7.1.5. Garantizar que el costo de la consultoría incluya todos y cada uno de los elementos, materiales y personal que sean necesarios para llevar a cabo la consultoría, y los respectivos entregables.
7.1.6. Asumir los costos derivados del transporte y seguros del personal para realizar las actividades en las Regionales y/o Centros Zonales
7.1.7. Asignar al proyecto el recurso humano idóneo y suficiente requerido para la consultoría.

## 7.2. Obligaciones generales

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

## 7.3. obligaciones del sistema de gestión de calidad

7.3.1. Todo el personal del contratista deberá estar afiliado al Sistema de Seguridad Social en riesgos laborales.
7.3.2. Durante la ejecución del contrato el contratista deberá cumplir con las normas reglamentarias sobre seguridad y salud en el trabajo, medicina preventiva, higiene y



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

seguridad industrial y los demás aspectos inherentes que han sido establecidos o establezca la ley y los organismos de control.

7.3.3. 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.

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

## 8. LUGAR DE EJECUCIÓN DEL CONTRATO

El lugar de ejecución del contrato será en la Sede de la Dirección General ubicado en la Avenida Carrera 68 No. 64C-75, de la ciudad de Bogotá y en las Regionales y/o Centros Zonales estipulados por el ICBF

## 9. PLAZO DE EJECUCIÓN

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

## 10. VALOR Y FORMA DE PAGO

El valor del servicio a suscribir será hasta por el valor resultante de la adjudicación, incluidos todos los costos directos e indirectos asociados a la prestación del servicio, el IVA, y demás impuestos de ley. El costo total del servicio incluye el correspondiente a los recursos humanos y demás costos indirectos necesarios para obtener todos los ítems definidos en el presente documento, de acuerdo con el plazo establecido.

Se pagará al contratista así: tres pagos cada uno cada uno del 33.33% del valor total del contrato, previa aprobación de los entregables de la fase correspondiente por parte del supervisor del contrato.

Los tres pagos se realizarán una vez se hayan terminado las fases así:

Primer Pago: Fase Diagnóstico de Seguridad y Fase de Análisis de Riesgos.

Segundo Pago: Fase de BCP – BIA – DRP y Fase de Normograma.

Tercer Pago: Fase Plan Estratégico Seguridad De La Información y Fase de Sensibilización Colaboradores ICBF.

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.

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.

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

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

## 11. ANEXOS

**11.1.** Anexo1- listado de regionales y/o centros zonales.
**11.2.** Anexo 2 – Fases de ejecución.

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

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

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



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