FICHA DE CONDICIONES TÉCNICAS ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DEL BIEN (FCT)	**Fecha**	19/11/2018

1. DENOMINACIÓN DEL BIEN O SERVICIO

Adquirir, configurar, parametrizar e implementar un software que permita realizar seguimiento y control a las gestiones que integran el Eje de Seguridad de la Información del ICBF.

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

43233200-Software de seguridad y protección.
43232300-Software de consultas y gestión de datos.
43233700-Software de administración de sistemas.

3. UNIDAD DE MEDIDA

Sistema de información

4. DESCRIPCIÓN GENERAL

El ICBF es un establecimiento público descentralizado, con personería jurídica, autonomía administrativa y patrimonio propio, creado mediante la Ley 75 de 1968 y su decreto reglamentario 2388 de 1979, adscrito al Departamento Administrativo para la Prosperidad Social, mediante Decreto 4156 de 2011, que tiene por objeto propender y fortalecer la integración y desarrollo armónico de la familia, proteger a los niños, niñas y adolescentes y garantizarles sus derechos.

De conformidad el artículo 22° del Decreto 987 de 2012, son funciones de la Dirección de Información y Tecnología, entre otras, las siguientes:

1. *Definir los requerimientos estratégicos de los sistemas de información de la Entidad.*
2. *Planear, desarrollar o solicitar la contratación a que haya lugar, de acuerdo con el procedimiento establecido, y mantener la infraestructura informática y de comunicaciones necesaria para la prestación de los servicios técnicos y administrativos de la Entidad.*
3. *Asesorar a la Dirección General en la definición de políticas, estrategias y lineamientos para el manejo de la información y desarrollo de los sistemas tecnológicos.*
4. *Verificar la integridad, disponibilidad y confidencialidad de la información de la Entidad.*
5. *Definir las metodologías, estándares, políticas y estrategias para el diseño, construcción y administración de los sistemas de información y uso de los recursos tecnológicos.*
6. *Proponer, planear y participar en estudios sobre las tendencias de las tecnologías de información.*

7. *Adquirir o construir los instrumentos tecnológicos y brindar el soporte para garantizar la captura de la información de los usuarios de los programas del ICBF a través del Registro Único de Beneficiarios (RUB).*
8. *Elaborar y presentar a la Dirección General el plan de adquisición, mantenimiento y distribución de hardware y software requerido por el Instituto.*
9. *Definir y hacer seguimiento a sus metas, planes de acción e Indicadores, en coordinación con la Dirección de Planeación y Control de Gestión y, el plan de compras y plan de contratación, en coordinación con la Dirección de Logística y Abastecimiento.*
10. *Coordinar con las Direcciones Regionales las actividades que sean de su competencia, en trabajo conjunto con la Oficina de Gestión Regional.*
11. *Asegurar la implementación, mantenimiento y mejora del Sistema Integrado de Gestión, en coordinación con la Dirección de Planeación y Control de Gestión.*
12. *Atender las peticiones y consultas relacionadas con asuntos de su competencia.*
13. *Preparar y presentar informes de seguimiento y gestión de los procesos a su cargo.*

(…)

Que el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Además, la Resolución 7070 del 16 de agosto de 2017, establece en el Título I, Capítulo I, artículo 1° la definición del Sistema Integrado de Gestión del Instituto Colombiano de Bienestar Familiar – ICBF como una herramienta gerencial que tiene como propósito promover y facilitar la mejora continua de la gestión del ICBF, orientada a lograr el impacto en los servicios que se prestan a los niños, niñas, adolescentes y familias colombianas, mediante la adopción de cuatro ejes (Calidad, Ambiental, Seguridad y Salud en el Trabajo y Seguridad de la Información), asimismo, establece en el Título III, Capítulo I, artículo 16° los Líderes de los Ejes del Sistema Integrado de Gestión – SIGE, delegando a la Dirección de Información y Tecnología como Líder del Eje de Seguridad de la Información.

Teniendo en cuenta lo anterior, el ICBF en su operación hace uso de las Tecnologías de Información y las Comunicaciones para el cumplimiento de su misionalidad, la cual consiste en "(…) *Trabajar con calidad y transparencia por el desarrollo y la protección integral de la primera infancia, la niñez, la adolescencia y el bienestar de las familias colombianas* (…)"; apoyado en los recursos tecnológicos propios y al servicio de la Entidad, para ello ha implementado un Sistema de Gestión de Seguridad de la información regulada mediante la Resolución 9674 de 2018, que establece el ámbito de aplicación en su artículo tercero, "*La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación y las Políticas Generales de Manejo aplica donde el Instituto Colombiano de Bienestar Familiar - ICBF tenga presencia o desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de*

información, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.", lo cual involucra a todas las sedes administrativas del ICBF, así como a las unidades de servicios contratadas con operadores sociales; de igual manera ha certificado en la NTC ISO 27001:2013 los 16 Procesos del Mapa de Operación por Procesos, en la Sede de la Dirección General y 16 Regionales (Antioquia, Atlántico, Bogotá, Bolívar, Caldas, Caquetá, Cauca, Córdoba, Magdalena, Nariño, Quindío, Risaralda, Santander, Sucre y Valle del Cauca); por lo anterior, se hace necesario gestionar el alto desempeño del Eje de Seguridad de la Información en la administración de alrededor de 12500 activos de información, 321 riesgos de Seguridad de la Información, 34 planes de continuidad de la operación, , Seguridad Digital o Ciberseguridad, Indicadores, Análisis de Brechas, que en la actualidad se gestionan a través de archivos de Excel.

Las anteriores cifras están sustentadas en la labor realizada por cada una de las gestiones que conforman al eje de seguridad de la información para las vigencias 2017 y 2018, decir se realizó un levantamiento y actualización de los activos de información, al igual que los riesgos l la elaboración de 34 planes de continuidad de la operación información que se encuentra publicada en la intranet de la Entidad.

De manera que requiere la adquisición , configuración , parametrización e implementación de un software de Seguridad de la Información que permita administrar, y gestionar los activos de seguridad de la información, incidentes de seguridad de la información, riesgos de seguridad de la información, Continuidad del Negocio (BCP), Seguridad Digital/Ciberseguridad, Declaración de Aplicabilidad (SOA), Análisis de Brecha (Análisis GAP), Matriz de Requisitos legales (Cumplimiento), Indicadores (estadísticas), documentación, políticas y las demás gestiones inherentes a un sistema de gestión de seguridad de la información basado en ISO 27001:2013, que sea valorado bajo la metodología PHVA.

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

- Ley 1712 de 2014
- Ley 1581 de 2012
- NTC ISO 27001:2013 Sistema de Gestión de Seguridad de la Información.
- NTC ISO 31000:2018 Riesgos.
- NTC ISO 22301:2012 Continuidad del negocio
- NTC ISO 27035:2012 Incidentes
- NTC ISO 27004:2016 Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Monitoreo, medición, análisis y evaluación.
- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano
- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
- Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, ("11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital)
- Resolución 8080 de 2016 se aprueba el Manual del Sistema Integrado de Gestión en el ICBF
- Resolución Interna 9674 de 2018 – Política de Seguridad y privacidad de la información, seguridad digital y continuidad de la operación.
- Resolución No. 6970 de 2018, integró y reglamentó el Comité Institucional de Gestión y Desempeño.
- Resolución 7070 de 2017 - Reorganiza el Sistema Integrado de Gestión.
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital del Departamento Administrativo para la Función Pública (DAFP) año 2018.

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

6.1. ESPECIFICACIONES GENERALES DEL SOFTWARE

- El sistema de información debe ser modular para el apoyo al ciclo PHVA de gestión de Seguridad de la Información.
- El licenciamiento debe ser OnPremise perpetuo para ICBF y no debe limitar la cantidad de usuarios del sistema.
- El aplicativo debe estar desarrollado para acceso y operación vía web, debe ser compatible con cualquier navegador del mercado en su última versión.
- Permitir la carga, consolidación, administración, automatización y reporte de información relacionada con la gestión realizada en un Sistema de Gestión de Seguridad de la información (SGSI).
- Debe proveer notificaciones, reportes de la realización de las actividades y de los resultados para la toma de decisiones.
- La versión del software desplegada en el ambiente de producción debe contar con una garantía mínima de un año sobre el correcto funcionamiento de la misma a partir del vencimiento el plazo de ejecución del contrato
- El software debe estar o poder configurarse en el idioma español.
- Debe ser compatible con protocolo LDAP para integrar el logueo con Directorio Activo de Microsoft o contar con la funcionalidad de Single Sign-On.
- Debe contar con un modulo de seguridad para gestionar la asignación de roles y privilegios para el acceso a los diferentes módulos solicitados en la Ficha de condiciones Técnicas.
- Debe poder configurase para gestionar el SGSI desde el nivel central, regional y zonal.
- El aplicativo debe poder configurar su gestor de bases de datos en los motores con los que cuenta la Entidad (SQL Server 2017 sin modo de compatibilidad a versiones inferiores o MySQL versión 5.7 o superior)

- El aplicativo debe ser en arquitectura multicapa, cada capa es un proceso separado y bien definido corriendo en plataformas separadas y debe poder configurarse en servidores Windows Server 2016 o Linux 7.5 Red Hat, es de resaltar que la infraestructura es proporcionada por la Entidad.
- El aplicativo debe ser compatible con ambientes virtualizados Hyper-V.
- El gestor de reportes debe estar incluido como modulo del sistema y debe ser propio del fabricante.
- Las notificaciones del sistema deben poder visualizarse a través de la aplicación y/o vía e-mail.
- El sistema debe ser multiusuario.
- Alinear el software con el Modelo de seguridad y privacidad de la información (MSPI), definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y contemplado en la política de la seguridad digital como habilitador trasversal..
- Realizar seguimiento a tareas y/o planes operativos y de implementación (gestión de proyectos).

- Realizar entrega de la siguiente documentación:
  - Manual de usuario del aplicativo.
  - Manual Técnico del aplicativo.
  - Ficha Técnica –Aplicaciones y bases de datos,
  - Diseño de Arquitectura física
  - Documento de arquitectura de software (que incluya modelo y diccionario de datos
  - Requerimientos de hardware y software (infraestructura mínima requerida para el desempeño óptimo de la aplicación
  - Instructivo de instalación y configuración del aplicativo.
  - Manual de Instalación y Configuración
  - Suscribir el acta de entrega del aplicativo.
  - Plan de Contingencia Sugerido

6.2. COMPONENTES O MODULOS DEL SOFTWARE

El Software de Seguridad de la información requerido por el ICBF, debe incluir los siguientes componentes funcionales (módulos):

- Administración y configuración
- Indicadores
- Gestión de Activos
- Gestión de Riesgos (identificación, tratamiento, evaluación y oportunidad de mejora)
- Administración y gestión de Incidentes
- Administración declaración de aplicabilidad
- Análisis GAP
- Continuidad del Negocio (BIA, Pruebas)
- Documentación.
- Seguridad digital (Ciberseguridad)

6.2.1. Funcionalidades de administración y configuración a través de las cuales se permita:

6.2.1.1. Crear y administrar grupos y perfiles de usuario, como mínimo administrador, transaccional y consulta, con opciones de acceso a los módulos, procesos, roles, documentación, pudiendo definir la responsabilidad de edición, consulta, eliminación, administración y generación de reportes.

6.2.1.2. Parametrizar los procesos en el componente de seguridad de la información, de acuerdo con el modelo de operación por procesos del ICBF el cual puede ser consultado en el siguiente dirección web https://www.icbf.gov.co/instituto/sistema-integrado-gestion/procesos.

6.2.1.3. Debe permitir configurar la autenticación de usuarios por directorio activo.

6.2.1.4. El sistema debe contar con una bitácora de auditoría relacionada con los accesos al sistema y las acciones realizadas por los usuarios para cada uno de los eventos que componen el aplicativo.

6.2.2. Módulo de indicadores que permita:

6.2.2.1. Definir, formular y administrar los indicadores con base en la norma ISO 27004:2016.

6.2.2.2. Definir los periodos sobre los cuales se va a realizar la medición, revisión y reporte de los indicadores.

6.2.2.3. Calificar el nivel de cumplimiento de los indicadores.

6.2.2.4. Permitir que los usuarios gestionen la información de los indicadores y se adicione información de seguimiento.

6.2.2.5. Guardar los registros de información y evidencia de quien realizó las calificaciones de indicadores y cuando se realizaron o actualizaron.

6.2.2.6. Representar gráficamente la información correspondiente a los indicadores.

6.2.2.7. Obtener los reportes de la gestión de indicadores con:

- Gráficas de resultados de la medición de indicadores.
- Hoja de vida de los indicadores.

6.2.3. Módulo de gestión de activos que permita:

6.2.3.1. La definición de los niveles que se van a utilizar para valorar las propiedades de confidencialidad, integridad y disponibilidad y otras propiedades que se requieran como trazabilidad o no repudio de los activos de información.

6.2.3.3. Parametrizar el esquema de clasificación de la información y personalizar la descripción de las escalas de valoración y clasificación de los activos de información de acuerdo con la metodología definida por ICBF (el sistema de información debe permitir soportar varias metodologías en relación con la gestión de activos de información), y debe incluir lo establecido en la Ley 1712 de 2014 y Ley 1581 de 2012.

6.2.3.4. Asociar los activos de información a cada uno de los procesos correspondientes al Modelo de Operación por Procesos , definida por el ICBF, para lo cual la Entidad realizara entrega de los mismos en archivo de Excel para su migración al aplicativo.

6.2.3.5. Identificar los activos de información que cuentan con datos personales y el tipo de dato de acuerdo con lo establecido en la Ley 1581 de 2012.

6.2.3.6. Identificar la dependencia de los activos con otros que se hayan registrado en el sistema.

6.2.3.7. Consultar activos de información específicos por cualquier criterio o combinando los campos de información asociados a los mismos.

6.2.3.8. Manejar los históricos de los cambios realizados a los activos de información.

6.2.3.9. Definir controles a los activos de información mediante un atributo que permita describir los controles asociados a cada uno de ellos.

6.2.3.10. Obtener de manera automatizada reportes acerca de:

- •Los resultados de los niveles de valoración de confidencialidad, integridad y disponibilidad asignados a los activos de información.
- •Los resultados de los niveles de clasificación asignados a los activos de información.
- •La matriz de inventario, valoración y clasificación de activos de información por procesos.

6.2.3.11. Exportar los reportes a formatos en Excel y PDF.

6.2.3.12 Identificar y asignar los propietarios y custodios de los activos.

6.2.3.13 Establecer la ubicación de los activos-

6.2.3.14 Establecer el tipo de activo (Físico, Electrónico, Software, Recurso Humano, Hardware, Soporte).

6.2.3.15 Parametrizar el activo de información con base en clasificación interna del ICBF y la Ley 1712 de 2014.

6.2.3.16 Parametrizar los atributos de continuidad, seguridad digital (ciberseguridad), de privacidad de cada activo de información.

6.2.3.17 Ingresar la descripción del activo de mínimo 200 caracteres.

6.2.3.18 Debe ser totalmente parametrizable (crear o quitar campos) de acuerdo con la dinámica de la gestión de activos.

6.2.3.19 Debe poder integrar con las demás gestiones del SGSI como lo son Incidentes, Riesgos y Continuidad.

6.2.4. Módulo de gestión de riesgos que permita:

6.2.4.1. Definir las escalas de valoración que se van a utilizar para medir el impacto (cualitativo y cuantitativo) , la probabilidad (cualitativo y cuantitativo), y los niveles de riesgos que va a tener la matriz, así como el mapa de calor que representan los niveles de riesgos y personalizar la descripción de estas escalas de valoración.

6.2.4.2. Carga y administrar los factores y causas de riesgo, vulnerabilidades y amenazas. La carga de esta información debe estar asociada a los tipos de

activos a los cuales aplica. Debe tener un catálogo de amenazas y vulnerabilidades precargado, administrable y clasificado por tipos de activos.

6.2.4.3. Registrar la información de identificación de factores, causas, amenazas, vulnerabilidades y controles existentes y la descripción del riesgo.

6.2.4.4. Realizar la valoración de los riesgos sobre los activos y actividades de los procesos determinando la probabilidad de ocurrencia, el impacto sobre los recursos del negocio, obteniendo automáticamente los niveles de riesgo que se hayan configurado en la metodología.

6.2.4.5. Definir el tratamiento de los riesgos, el sistema debe permitir seleccionar los controles para el tratamiento y poder generar un registro histórico de tratamiento de riesgos para el seguimiento de la implementación y medición de cada uno de los controles.

6.2.4.6. Definir y publicar desde la administración del sistema, formularios que contengan campos nuevos y adicionales a los que trae por defecto la solución, que se requieran tener sobre los riesgos.

6.2.4.7. Consultar riesgos específicos, mediante diversos criterios que permiten tomar decisiones y entender mejor la naturaleza de los riesgos.

6.2.4.8. El sistema debe permitir manejar riesgos de proceso y riesgos asociados a los activos de información.

6.2.4.9. El sistema debe permitir medir la efectividad de los controles asociados a los riesgos.

6.2.4.10. Debe manejar un histórico de todas las evaluaciones de riesgo realizadas por cada registro de riesgo.

6.2.4.11. Debe manejar un histórico de todos los seguimientos a los controles de los riesgos realizadas por cada registro del control.

6.2.4.12. Obtener como mínimo los siguientes reportes de datos y gráficos acerca de:

- Matrices gráficas en mapas de calor del riesgo inherente y residual, mostrando los datos que dan origen a la matriz. Se debe permitir exportar estos resultados a formatos en Excel y PDF incluyendo datos y gráficos.
- Niveles de riesgos por cada recurso del negocio.
- Top de vulnerabilidades, amenazas, activos con mayores riesgos.
- Top de causas y factores de riesgo.
- Informe gráfico de la evolución del riesgo, saber en dónde estaba el riesgo inherente y donde se encuentra actualmente el último riesgo residual.
- Informe de plan de tratamiento de riesgos, en donde se presenten los riesgos y la información de sus controles asociados.

6.2.4.13. El sistema debe permitir el registro de los tratamientos de los riesgos para poder establecer la materialización de los riesgos y contar con un registro histórico de los mismos.

6.2.4.14 Debe permitir la Clasificación de riesgos por diversos criterios.

6.2.4.15 Debe permitir parametrización de procesos, objetivos, contextos internos externos.

6.2.4.15 Debe permitir relacionar los Activos de información afectados con la materialización del riesgo

6.2.4.16 Debe permitir registrar la información de identificación de consecuencias positivas y negativas
6.2.4.17 Debe permitir seleccionar las opciones de tratamiento del Riesgo.
6.2.4.18 Debe permitir la evaluación de controles existentes e implementados
6.2.4.19 Debe permitir realizar seguimiento a los avances y estado actual de tratamiento del riesgo.
6.2.4.20 Debe permitir adjuntar a cada actividad del plan de tratamiento del riesgo los entregables y/o evidencias de su gestión o cumplimiento.
6.2.4.21 Debe permitir relacionar a cada riesgo las oportunidades de mejora una vez realizado el riesgo residual.
6.2.4.22 Mantener y consultar todos los registros históricos de las diferentes calificaciones del riesgo y del seguimiento de los niveles de riesgo residuales.
6.2.4.23 Debe permitir la Priorización del Riesgo de acuerdo a su criticidad correspondiente al nivel inherente. .
6.2.4.24 Debe permitir la parametrización de los criterios de afectación que tendría si ocurre la materialización del riesgo.
6.2.4.25. Debe poder integrar con las demás gestiones del SGSI.
6.2.4.26. Conocer cuales controles de seguridad están asociados a los activos y riesgos registrados en el sistema.

6.2.5. Módulo de administración y gestión de incidentes que permita:

6.2.5.1. Definir las escalas de valoración que se van a utilizar para medir la criticidad (Alto, Medio y Bajo), tiempo oportuno de atención definidos por la Entidad (0-2 horas alto, 0-4 horas Medio, 0-8 horas Bajo) y priorización de los incidentes según escala de 1 a 5 y personalizar la descripción de estas escalas de valoración
6.2.5.2. Configurar la gestión de incidentes basados en la ISO 27035:2012
6.2.5.2. Definir los tipos de incidentes y eventos que se van a manejar en el proceso de gestión de incidentes.
6.2.5.3. Permitir el manejo de evidencia del tratamiento del incidente y almacenarlo en el sistema.
6.2.5.4. Definir a quien se le comunica acerca de la ocurrencia y gestión de los incidentes a través de correo electrónico.
6.2.5.5.
6.2.5.6. Administrar la información del proceso de identificación, valoración y tratamiento de los incidentes, seleccionando los activos afectados y los riesgos que se materializan por el incidente.
6.2.5.7. Guardar los registros de información y evidencia que soportan el desarrollo de las actividades de tratamiento realizadas de contención, erradicación y recuperación del incidente.
6.2.5.8. Realizar el registro de las lecciones aprendidas KBD – Base de datos del conocimiento.
6.2.5.9. Realizar la consulta del estado de los incidentes y realizar las acciones de cierre de estos.

6.2.5.10. Obtener los reportes de la gestión de incidentes en cuanto:
• Histórico de incidentes.
• Top de incidentes por tipo (Seguridad de la Información, privacidad de Información, Seguridad Digital), activos afectados, criticidad , riesgos relacionado, usuarios afectados.
• Detalle de los incidentes por estado.
• Reporte detallado, gráficos de toda la información de los incidentes (identificación, valoración, tratamiento, costo del incidente) en Excel o PDF

6.2.5.11. Envío automático de alertas y notificaciones a los responsables.

6.2.5.12. Costear incidentes.

6.2.5.13. Debe poder integrar con las demás gestiones del SGSI

6.2.6. Módulo Administración declaración de aplicabilidad que permita:

6.2.6.1. Definir y administrar los niveles de madurez, del Sistema de Gestión de Seguridad de la Información.

6.2.6.2. Definir y administrar la Declaración de aplicabilidad del Sistema de Gestión de Seguridad de la Información.

6.2.6.3. Definir y administrar los objetivos de Control y controles que se encuentren implementados y operando, también los que hayan sido descartados.

6.2.6.4. Asociar si el control se debe implementar en el nivel Nacional, regional o Zonal.

6.2.6.5. Asociar evidencias de cumplimiento de cada control (Texto y archivos) o enlazar con documentos del módulo de documentación del aplicativo.

6.2.7. Módulo Administración GAP que permita:

6.2.7.1. Administrar los análisis GAP por los dominios de la norma ISO 27001:2013.

6.2.7.2. Administrar los análisis GAP por los objetivos de control.

6.2.7.3. Contar con las herramientas visuales para toma de decisiones de acuerdo con los GAPs.

6.2.7.4. Previsualización de los dominios y objetivos de control, implementados de la norma ISO 27001:2013 en el SGSI y las actividades que se deben hacer para implementar los faltantes.

6.2.8. Módulo de Documentación que permita:

6.2.8.1. CargarAdministrar los documentos que hagan parte del Sistema de Gestión de Seguridad de la Información y manejar versionamiento de los mismos.

6.2.9 Módulo de Continuidad de Negocio que permita:

6.2.9.1 Definir y realizar análisis de impacto al negocio (BIA), que contemple cálculos de MTPD, RTO, RPO e identificación y priorización de los procesos críticos de la entidad.

6.2.9.3 Definir escenarios de interrupción de las operaciones de los procesos críticos de la entidad, gestión de incidentes, DRP, y planes de continuidad de negocio.
6.2.9.4 Gestión de crisis, levantamiento, análisis y revisión de la continuidad.
6.2.9.5 Gestor documental, informes, formatos y tablas gráficas.
6.2.9.6 Gestionar las pruebas de todos los planes de continuidad del negocio del nivel central y regional.

6.2.10 Módulo de Seguridad Digital (Ciberseguridad) que permita:

6.2.10.1 Integración con los módulos de gestión de activos, riesgos e incidentes, con el fin de alinear el sistema en estándares y buenas prácticas en Ciberseguridad.

7. OBLIGACIONES DEL CONTRATISTA

7.1. Obligaciones específicas

7.1.1. Cumplir con plena autonomía técnica y administrativa, con las actividades, lineamientos y estándares definidos en el numeral 6 “Especificaciones Técnicas de los insumos, bienes, productos, obras o servicios a entregar” de la Ficha de Condiciones Técnicas Esenciales para la Prestación del Servicio y/o Entrega del Bien (FCT).
7.1.2. Instalar, configurar, parametrizar y poner en funcionamiento el software web que permita realizar seguimiento y control a las gestiones que integran el Eje de Seguridad de la Información del ICBF.
7.1.3. Garantizar el cumplimiento de las características de seguridad del software.
7.1.4. Entregar dentro de los dos (2) días hábiles siguientes al cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, un cronograma detallado de la ejecución del objeto contractual, el cual deberá ser aprobado por el supervisor del contrato.
7.1.5. Entregar los manuales de administración y de usuarios de todos los módulos del sistema ofrecido en formato PDF o HTML, y en el idioma español
7.1.6. Entregar documento de licenciamiento del software con las condiciones específicas del licenciamiento exigidas por ICBF en Ficha de Condiciones Técnicas Esenciales para la Prestación del Servicio y/o Entrega del Bien (FCT).
7.1.7. Realizar transferencia de conocimiento al equipo de Seguridad de la Información o a quien disponga el supervisor del contrato, para lo cual debe generar los respectivos soportes. Los temas a tratar deben contener la funcionalidad y configuración de cada módulo adquirido, administración de roles y perfiles, generación de reportes, generación de indicadores, actualización catálogo (amenazas y sus consecuencias), para lo cual el proveedor debe disponer de un total de 24 horas.
7.1.8. Realizar pruebas de funcionamiento antes de la puesta en producción de cada uno de los módulos adquiridos en el ambiente que el ICBF determine para tal fin, para lo cual se establecerá un guion de pruebas con el fin de recibir en correcto funcionamiento los módulos adquiridos y sus integraciones.

7.1.9. Brindar soporte técnico durante el plazo de ejecución del contrato, en jornada 5 X 8, para lo cual deberá disponer de uno o varios de los siguientes canales de atención: contacto telefónico, correo electrónico, mesa de servicio y de ser requerido el soporte será brindado en sitio.

7.1.10. Hacer entrega del certificado de garantía del software por parte del fabricante por el periodo de un año contado a partir del despliegue en producción de la aplicación

7.1.11. Migrar los activos de información por cada uno de los procesos suministrados por la entidad en archivo de Excel.

7.2. Obligaciones generales

7.2.1. Cumplir con el objeto del contrato con plena autonomía técnica y administrativa y bajo su propia responsabilidad, por lo tanto, no existe ni existirá ningún tipo de subordinación, ni vínculo laboral alguno entre EL CONTRATISTA o su personal y el ICBF.

7.2.2. Constituir y allegar a EL ICBF las garantías requeridas dentro de los tres (3) días hábiles siguientes a la suscripción del contrato.

7.2.3. Participar y apoyar a EL ICBF en todas las reuniones a las que éste lo convoque relacionadas con la ejecución del contrato.

7.2.4. Disponer de los medios necesarios para el mantenimiento, cuidado y custodia de la documentación objeto del presente contrato.

7.2.5. Atender los requerimientos, instrucciones y/o recomendaciones que durante el desarrollo del Contrato le imparta EL ICBF a través del supervisor del mismo, para una correcta ejecución y cumplimiento de sus obligaciones.

7.2.6. Entregar al supervisor del Contrato los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos cuando así se requiera.

7.2.7. Presentar la factura de conformidad con la forma de pago estipulada en el contrato, junto con el informe de las actividades realizadas para cada pago.

7.2.8. Guardar estricta reserva sobre toda la información y documentos que tenga acceso, maneje en desarrollo de su actividad o que llegue a conocer en desarrollo del contrato y que no tenga carácter de pública. En consecuencia, se obliga a no divulgar por ningún medio dicha información o documentos a terceros, sin la previa autorización escrita del ICBF.

7.2.9. Mantener correctamente actualizados cada uno de los sistemas de información que maneje en desarrollo de su actividad.

7.2.10. Asumir un buen trato para con los demás colaboradores internos y externos del Instituto Colombiano de Bienestar Familiar, y actuar con responsabilidad, eficiencia y transparencia.

7.2.11. Devolver al ICBF, una vez finalizado la ejecución del contrato los documentos que en desarrollo del contrato se hayan producido, e igualmente todos los archivos que se hayan generado en cumplimiento de sus obligaciones.

7.2.12. Colaborar con el ICBF en el suministro y respuesta de la información correspondiente, a los requerimientos efectuados por los organismos de control del Estado Colombiano en relación con la ejecución, desarrollo o implementación del contrato objeto del presente documento.

7.2.13. Utilizar la imagen del ICBF de acuerdo con los lineamientos establecidos por éste. Salvo autorización expresa y escrita de las partes, no se podrá utilizar el nombre, emblema o sello oficial de la otra parte para fines publicitarios o de cualquier otra índole.

7.2.14. Realizar los pagos al SISS (salud, pensión y riesgos laborales) y parafiscales, de acuerdo con la normatividad vigente aportando los soportes de pago correspondientes.

7.2.15. Respetar la política medioambiental del ICBF, política que incluye todas las normas internas sobre el uso de los recursos ambientales, como el agua y la energía, racionamiento de papel, norma sobre parqueaderos y manejo de desechos residuales.

7.2.16. Cumplir con las disposiciones establecidas en el Capítulo “Buenas Prácticas en la Gestión Contractual” del Manual de Contratación vigente.

7.2.17. Remitir al supervisor del contrato, dentro de los tres (3) días siguientes a la consignación, copia del documento donde conste la operación que, por concepto de reintegros, rendimientos financieros, multas o cualquier otro, se causen a favor de la Entidad en razón a la ejecución del contrato. PARÁGRAFO: Las consignaciones a que hace referencia esta obligación deben realizarse únicamente en la cuenta informada por escrito por el supervisor del contrato.

7.3 Obligaciones del Sistema Integrado de Gestión

7.3.1 Obligaciones del Eje de Gestión de Calidad:

7.3.1.1 Demostrar que selecciona y evalúa sus proveedores de bienes y servicios, relacionados directamente con la prestación del servicio contratado, haciendo cumplir las normas legales vigentes, así como las normas y especificaciones técnicas según corresponda.

7.3.1.2 Determinar un mecanismo para conocer la percepción del beneficiario frente a la prestación del servicio, a través de un instrumento establecido por el mismo operador para tal fin.

7.3.1.3 Demostrar mediante evidencias la implementación de acciones de mejora (correctivas o preventivas frente a cualquier situación que afecte la prestación del servicio)que permita tomar las decisiones a que haya lugar o experiencia exitosas que de muestren la mejora en la prestación de servicio

7.3.2 Obligaciones del Eje de Seguridad de la Información:

7.3.2.1 Suscribir un documento de compromiso de confidencialidad el cual deberá ser entregado al supervisor del contrato una vez se firme el contrato.
7.3.2.2 Informar al supervisor, en el momento que ocurran incidentes de seguridad que afecten la disponibilidad, integridad y/o confidencialidad de la información del ICBF, en el marco de la ejecución del contrato.

7.3.3 **Obligaciones del Eje de Seguridad y Salud en el Trabajo:**

7.3.3.1 Garantizar que todos los colaboradores vinculados para la ejecución del contrato o convenio se encuentren afiliados al Sistema de Seguridad Social, incluido los riesgos laborales.

7.3.4 **Obligaciones del Eje de Gestión Ambiental:**
N/A

8. LUGAR DE EJECUCIÓN DEL CONTRATO

El lugar de ejecución del contrato será en Bogotá D.C.

9. PLAZO DE EJECUCIÓN

El plazo ejecución será a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato hasta el 30 septiembre del 2019.

10. FORMA DE PAGO DEL VALOR DEL CONTRATO

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

Se pagará al contratista así:

Un (1) único pago, relacionado con el cumplimiento de todas las obligaciones pactadas en el numeral 6, en relación con la entrega, configuración, parametrización e implementación del software de Seguridad de la Información en un ambiente de producción, y al recibo a satisfacción por parte del supervisor.

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.

11. TIPIFICACIÓN, VALORACIÓN 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 el Anexo No. **01 Matriz de identificación, valoración y asignación de riesgos**, 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 anexo **No. No. 01 Matriz de identificación, valoración y asignación de riesgos.**

Los riesgos que podrían afectar el normal desarrollo de las actividades previstas en esta contratación se analizan en el anexo **No. 01 Matriz de identificación, valoración y asignación de riesgos**, elaborado de acuerdo con la metodología propuesta por Colombia Compra Eficiente (CCE) detallada en el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación".[1]

12. ANEXOS

Anexo No. 1 Matriz de identificación, valoración y asignación de riesgos
Anexo N0. 2 Guía para el Desarrollo de Inventario y Clasificación de Activos

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.

14. APROBACIONES ICBF

Concepto	Nombre y apellidos	Cargo – Dependencia	Firma
Elaboró	Fabián Andrés Burgos Suárez	Contratista SGSI - DIT	

[1] Agencia Nacional para la Contratación Pública – Colombia Compra Eficiente, disponible en www.colombiacompra.gov.co, https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documents/cce_manual_cobertura_riesgo.pdf, fecha de consulta 26 de abril de 2018.

Concepto	Nombre y apellidos	Cargo – Dependencia	Firma
Elaboró	Sergio Andres Ramos	Contratista SGSI - DIT	
Revisó	Andrés Diaz Molina	Contratista Líder SGSI – DIT	
Revisó	Camilo Gutierrez	Subdirector de Sistemas Integrados de Información	
Revisó	Karen Gutierrez	Contratista - DIT	
Aprobó	Piedad Cecilia Montero	Directora de Información y Tecnologia- DIT	