Términos de Referencia

"Solución informática para el procesamiento, validación y divulgación de estados financieros e informes de auditoría, sobre plataforma XBRL"

Marco Estratégico

Los distintos actores del sistema económico de un país constantemente se enfrentan a la necesidad de tomar decisiones cuyo impacto es de significativa relevancia, tanto para el interés público como privado. Para que el poder público pueda tomar medidas económicas, y para que las empresas puedan tomar decisiones de negocio, es fundamental que se cuente con sistemas de información confiables. Estos sistemas, requieren que la información contenida en ellos cumpla con varios atributos, como ser: pertinencia, confiabilidad, sistematicidad, comparabilidad, claridad y relevancia, entre otros.

Las empresas argentinas deben presentar su información financiera ante distintos organismos y entidades. La periodicidad con que deben cumplir dicha obligación depende de factores como los requerimientos establecidos en normativa contable e impositiva o las necesidades de reporte de cada empresa, entre otros.

Actualmente, no existen bases sistematizadas, ni con datos agregados, que permitan efectuar análisis puntuales o sobre información consolidada. Asimismo, no hay traspaso de información financiera (por ejemplo, balances) de las empresas entre los distintos organismos públicos o privados, por lo que la misma queda dispersa y sumergida en la burocracia administrativa.

Esta falta de homogeneidad y dispersión en la información:

- Dificulta el análisis sectorial o de mercado, lo cual es de suma relevancia en un contexto donde la política económica del país tiene entre sus principales objetivos atraer inversión extranjera.
- Limita la posibilidad de tomar decisiones de negocios con fundamentos sólidos.
- Complejiza la adopción de las mejores prácticas y tendencias globales de transformación financiera (i.e. negocios basados en fintech), imposibilitando a las empresas aprovechar las eficiencias y ahorros que ello conlleva.

En lo que respecta a la Administración Pública Nacional, dicha información reviste carácter esencial en vistas al ejercicio de prerrogativas constitucionales tales como promover la industria, el progreso económico y la productividad de la economía nacional. Sin información suficiente y confiable, la adopción de políticas de estado en estas cuestiones puede resultar infructuosa.

Por otra parte, si se analizan estas cuestiones desde el punto de vista del sistema financiero, la falta de información es uno de los factores que contribuyen a generar

importantes costos operativos y de gestión del riesgo, afectando fundamentalmente el otorgamiento de financiamiento al sector MIPyME. Teniendo en consideración que más del 95% de las empresas del país entran en dicha categoría, esta situación tiene un alto impacto negativo en el nivel de inversión productiva del país y, por consiguiente, en el nivel de desarrollo.

En los últimos 30 años el mundo ha experimentado una revolución tecnológica en términos de conectividad que ha disminuido drásticamente los costos de acceso a la información. Estos cambios tecnológicos han cambiado profundamente la manera de dimensionar y poner precio al riesgo, aumentando significativamente la competencia e incentivando a los proveedores de capital a explorar nuevos horizontes para hacer negocios y, como resultado, incrementado exponencialmente la penetración crediticia mundial. Por diversos motivos, este proceso no ha sucedido en Argentina, hasta ahora.

De acuerdo con datos publicados por el Banco Mundial (Global Financial Development Database), la penetración del crédito privado dado por bancos y otras instituciones financieras en Argentina es una de las más bajas del mundo, y la más baja de la región. En 2005, dicho indicador representaba el 9% del PBI (cuando el promedio de la región rondaba el 27%), mientras que en 2016 llegaba al 12%, (contra un promedio regional del 50%).

En este contexto, surge por iniciativa conjunta del Ministerio de Producción y Trabajo (en adelante también el "Ministerio") y la Federación Argentina de Consejos Profesionales de Ciencias Económicas (en adelante también "FACPCE") la idea de crear la Central Federal de Información Financiera (en adelante también "CenFIF") que tenga por objeto la consolidación de toda la información contable, fiscal y financiera de todo el ecosistema empresarial argentino mediante la utilización de taxonomías estandarizadas de presentación en formato XBRL.

El propósito de esta entidad será promover el acceso a información de calidad para distintos usuarios a los efectos de:

- Brindar transparencia.
- Proveer herramientas para brindar sustentabilidad al sistema financiero al contribuir a la disminución de los costos operativos y de gestión del riesgo.
- Configurar un mejor ecosistema de negocios.
- Facilitar la toma de decisiones fundadas.
- Facilitar herramientas para el acceso al crédito y la inversión productiva.

En el marco de este proyecto, el Ministerio, con el apoyo del Proyecto de Acceso a Financiamiento a más Largo Plazo para MIPYMEs (BIRF N°159515), Préstamo N° 8659-AR firmado entre la República Argentina y el Banco Internacional de Reconstrucción y Fomento el 20 de abril de 2018, ha iniciado la búsqueda e identificación de potenciales proveedores que presten un servicio de asesoramiento integral que incluya la **provisión de una solución informática** (en adelante *una Plataforma*) **que permita la recepción, el procesamiento, la validación y la divulgación de los estados financieros de las entidades informantes y sus informes de auditoría, basados en documentos instancia XBRL**.

Producto Requerido

I. Objeto

Se requiere un servicio de asesoramiento integral que incluya la provisión de una solución informática (en adelante *una Plataforma*) que permita la recepción, el procesamiento, la validación y la divulgación de los estados financieros de las entidades informantes y sus informes de auditoría, basados en documentos instancia XBRL.

Adicionalmente se requieren todos los servicios vinculados para la implementación, personalización, puesta en marcha, puesta a punto, soporte funcional y técnico, capacitación, provisión de documentación y mantenimiento.

II. Alcance

A continuación, se detalla el desglose mínimo requerido de la estructura de trabajo del proyecto:

EDT[1]	**Paquetes de Trabajo**
Inicio del Proyecto	▪ Actividades preparatorias. ▪ Capacitación orientada al análisis de brechas. ▪ Desarrollo del plan de trabajo utilizando metodologías ágiles.
Diagnóstico, Análisis y Diseño	▪ Documentación de los requerimientos de funcionales, no funcionales y de soporte y mantenimiento de alto nivel. ▪ Análisis de brechas funcionales y técnicas y diseño de los *sprints.* ▪ Planificación de los *sprints.* ▪ Definición del tipo de integración con **FIRMA DIGITAL de AFIP.** ▪ Definición del tipo de integración con el ERP (CRM, Help Desk y Contable)**.** ▪ Plan de aceptación de pruebas (aseguramiento de la calidad).
Implementación	▪ Desarrollo, configuración y parametrización en detalle de los requerimientos funcionales, no funcionales y de soporte y mantenimiento. ▪ Desarrollo de la integración con **FIRMA DIGITAL de AFIP.** ▪ Desarrollo de la integración con el ERP (CRM, Help Desk y Contable)**.** ▪ Ejecución del plan de aceptación de pruebas. ▪ Servicio de capacitación. ▪ Provisión de documentación.
Pilotos	▪ Planificación y ejecución de pilotos. ▪ Evaluación del funcionamiento de los pilotos. ▪ Ajustes, refinamiento, readecuación, reconfiguración, recambio de parámetros, ajuste de la documentación y recapacitación fruto de los resultados de la ejecución de los pilotos. ▪ Aseguramiento de la calidad.

[1] *Estructura Desglosada de Trabajo*

EDT[1]	Paquetes de Trabajo
Puesta en Producción	▪ Actividades de cierre. ▪ Puesta en producción final.
Soporte y Mantenimiento (Implementación y Post-Producción)	▪ *Help Desk* para consultas. ▪ Primer y segundo nivel de soporte. ▪ Soporte virtual. ▪ Mantenimiento correctivo, preventivo y evolutivo.

Se requiere que la Plataforma sea un sistema integrado que permita la recepción, el procesamiento, la validación y la divulgación de los estados financieros de las entidades informantes y sus informes de auditoría, basados en documentos instancia XBRL, preparados de acuerdo con las siguientes taxonomías basadas en la Taxonomía NIIF 2018:

- Taxonomía NIIF.
- Taxonomía Grandes Empresas bajo normas Argentina.
- Taxonomía Medianas Empresas bajo normas Argentina.
- Taxonomía Pequeñas Empresas bajo normas Argentina.

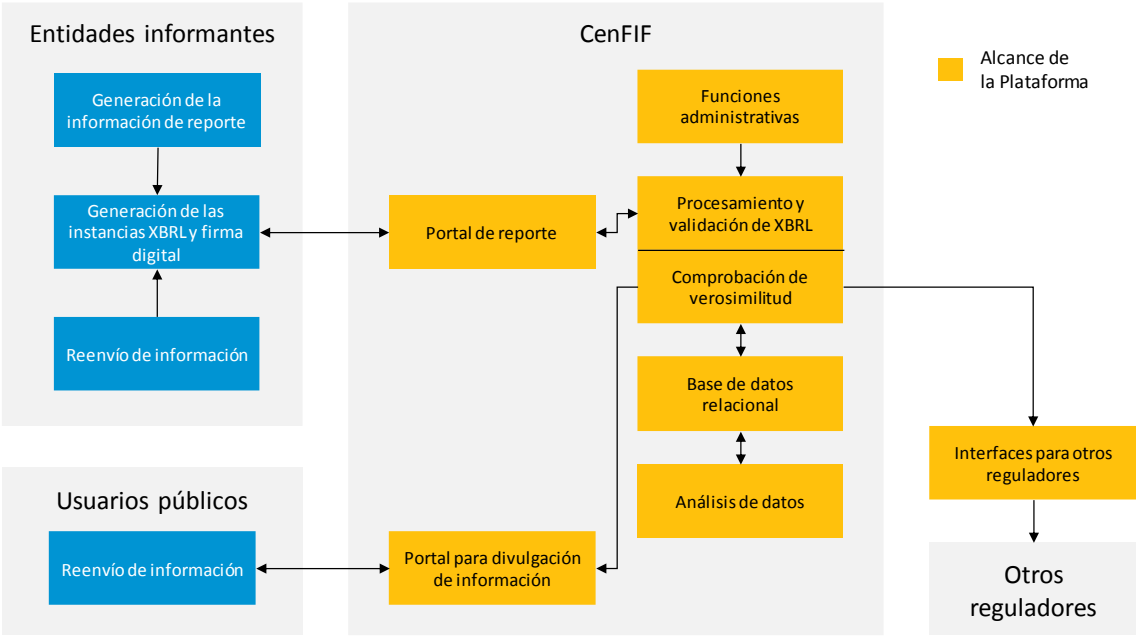
Las características y necesidades mínimas que deberán ser cubiertas por la Plataforma son:

- La Plataforma deberá permitir la creación, administración y publicación de Taxonomías XBRL.
- La Plataforma deberá permitir la recepción de documentos instancia en XBRL, Excel, CSV, XML y vía Web, preparados por las entidades informantes, de acuerdo con las Taxonomías XBRL.
- La Plataforma deberá permitir el procesamiento y la validación de documentos instancia en XBRL, Excel, CSV y XML y vía Web, según las reglas de validación definidas para las Taxonomías XBRL.
- La Plataforma deberá permitir el procesamiento y almacenamiento de documentos instancia en XBRL.
- La Plataforma deberá permitir la conversión de los datos de los documentos instancias en XBRL a documentos Excel, CSV, XML y PDF.
- La Plataforma deberá permitir la conversión de los datos de los documentos instancias en XBRL para su exportación a una base de datos relacional para permitir el análisis de los datos.
- La Plataforma deberá proporcionar a los usuarios de CenFIF la capacidad de monitorear el estado del cumplimiento de los requisitos de información de las entidades informantes.
- La Plataforma deberá proporcional a los usuarios de los Consejos Profesionales de Ciencias Economías (“CPCE”) acceso para realizar las certificaciones de los estados contables dentro del proceso de validación.
- La Plataforma deberá proporcionar a las entidades informantes la posibilidad de verificar el estado actual de sus presentaciones.

- La Plataforma deberá permitir a usuarios externos acceder a la información financiera de las entidades informantes siguiendo las reglas de divulgación definidas por CenFIF, en formato XBRL, Excel, CSV, XML y PDF.
- La Plataforma deberá proporcionar acceso a los usuarios de las entidades informantes, de los CPCEs y usuarios externos mediante FIRMA DIGITAL de AFIP.
- La Plataforma deberá seguir las mejores prácticas internacionales de gestión de datos, desarrollo y mantenimiento, recuperación ante desastres, eficiencia, confiabilidad, seguridad, usabilidad y otros requisitos operativos para un regulador de servicios financieros.

El siguiente diagrama representa las funciones principales y los componentes de la Plataforma:

Arquitectura de la Central Federal de Información Financiera



III. Exclusiones del Proyecto

No se requerirá la provisión de los siguientes bienes y servicios:

- Provisión del *hardware y el hosting* necesario para la implementación del entorno tecnológico de producción.

Para las tareas de instalación de los servidores y administración de sistemas operativos, la consultora deberá asesorar y especificar el tipo de hardware, software y sus requerimientos para que la solución funcione adecuadamente.

Sin embargo, la consultora podrá presentar de manera opcional una propuesta de Infraestructura como Servicio por separado para todos los entornos de la Plataforma

siguiendo los estándares de la Oficina Nacional de Tecnologías de Información (ONTI)[2] que será tenida en consideración a la hora de realizar la evaluación técnica.

IV. Restricciones del Proyecto

El proyecto deberá dar cabal cumplimiento a los siguientes aspectos normativos actualmente en vigencia o, los que eventualmente los reemplacen o complementen:

- Artículo 121 y concordantes de la Constitución Nacional en lo que respecta a facultades no delegadas por las provincias al gobierno nacional.
- Ley Nacional N° 25.326 de Protección de los Datos Personales.
- Ley Nacional N° 11.683, sobre Secreto Fiscal.
- Ley Nacional N° 26.831, sobre Secreto Bancario de entidades comprendidas dentro del Mercados de Capitales argentino.
- Ley Nacional N° 21.526, Secreto Bancario y Financiero.
- Ley Nacional N° 27.275, sobre Secreto Comercial.
- Ley Nacional N° 20.091, sobre Secreto de Entidades de Seguros.
- Ley Nacional N° 24.766, sobre secreto de información bajo el control de una persona, divulgada de manera contraria a usos comerciales.
- Ley Nacional N° 26.047 de constitución del Registro Nacional de Sociedades.
- Demás legislación y normas constitucionales o de jerarquía constitucional que amparen la propiedad y disposición de información privada, ya sea por su carácter personal o comercialmente sensible o por encontrarse relacionada con otros derechos amparados por la Constitución Nacional.
- Comunicación “A” 4609 del BCRA.
- Comunicación “A” 6354 del BCRA.
- Decreto 87/2017 del Ministerio de Modernización
- Disposición 02/2014 de Oficina Nacional de Tecnologías de Información (ONTI) para la aplicación de las Pautas de Accesibilidad Web 2.0[3]

La consultora y todo su personal involucrado, excepto previo consentimiento por escrito del **Ministerio**, no podrán revelar en ningún momento a cualquier persona o entidad ninguna información confidencial adquirida en el curso de la prestación de los servicios; ni la consultora ni su personal podrán publicar las recomendaciones formuladas en el curso de, o como resultado de la prestación de los servicios.

V. Supuestos del Proyecto

- Los lugares de desarrollo del proyecto serán las instalaciones del **Ministerio**. No obstante, si así lo requiriese, el **Ministerio** podrá solicitar que las reuniones que

[2] https://www.argentina.gob.ar/onti/estandares-tecnologicos/infraestructura-como-servicio

[3] http://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/233667/norma.htm

deban realizarse para las distintas actividades previstas en el proyecto, sean realizadas en la/s dependencia/s de la consultora, previo consenso.

- El **Ministerio** o quien designe, pondrá a disposición del proyecto un *Project Manager* para el seguimiento, el aseguramiento de la calidad y el cumplimiento de los plazos establecidos en el proyecto, quien será el interlocutor con el Gerente de Proyecto por parte de la consultora.
- El **Ministerio** o quien sea designado para tal fin, pondrá a disposición personal como contraparte del proyecto. Oportunamente, en la propuesta a presentar, la consultora deberá sugerir a su mejor saber y entender, las necesidades de roles y perfiles de los miembros del equipo que considere apropiado para el desarrollo del proyecto. De esta manera, junto con el *Project Manager* del **Ministerio**, se configurará el equipo del proyecto más apropiado para su ejecución.
- Se configurará una estructura de **PMO** para este proyecto que será integrada y liderada por el *Project Manager* del **Ministerio**.
- En lo referido a los entornos tecnológicos donde será instalada la Plataforma provista por la consultora para producción, el hardware y el hosting estarán a cargo del **Ministerio**. No obstante, la consultora deberá participar activamente en dicha tarea, asesorando y recomendando acerca de las características particulares que podrían necesitar dichas tareas para el correcto funcionamiento la Plataforma provista por ella.
- En lo referido al aseguramiento de la calidad, el **Ministerio** aportará al proyecto un equipo de profesionales para la homologación de las configuraciones, parametrizaciones y desarrollos de la Plataforma provista por la consultora para la implementación de este proyecto. Dicho equipo de profesionales será quién realice un informe no vinculante sobre las pruebas de los entregables del proyecto en función de los resultados de los planes de aceptación. No obstante, la consultora deberá realizar las mismas actividades de aseguramiento de la calidad, previo a la entrega al personal del **Ministerio** para la ejecución de las homologaciones, con el objetivo de eliminar tempranamente los problemas de calidad que puedan presentarse en las distintas etapas de pruebas (unitarias, de integración y de usuarios).
- Será obligación quién resulte adjudicatario de los productos y servicios requeridos, la completa y total observancia de los Estándares Tecnológicos dictados por la Oficina Nacional de Tecnologías de Información (ONTI)[4] y cumplir con los estándares definidos en la reglamentación del Decreto 87/2017 del Ministerio de Modernización y con la Disposición 02/2014 de ONTI para la aplicación de las Pautas de Accesibilidad Web 2.0.
- En el supuesto que se descontinúe la relación contractual entre el **Ministerio** y la consultora, esta última deberá entregar la totalidad de archivos de datos, bases de datos, u otros archivos que se hayan generado en el marco de la relación contractual. Asimismo, la consultora no podrá usar, conservar, divulgar o reproducir ningún dato del **Ministerio** ni cualquier otra información relacionada que se encuentren en sus sistemas informáticos o medios de

[4] https://www.argentina.gob.ar/modernizacion/estandarestecnologicos

almacenamiento que haya utilizado para llevar a cabo la implementación del proyecto.

VI. Software

Los oferentes deberán proveer una licencia perpetua de uso para un número ilimitado usuarios, tanto internos como externos.

La consultora y el **Ministerio** firmarán un acuerdo de código fuente con modalidad **ESCROW**, cuyo objetivo será garantizar que, en el caso de un cese permanente del soporte a la Plataforma, CenFIF disponga del último código fuente de la Plataforma y las personalizaciones relacionadas.

El acuerdo debe garantizar que el código fuente (junto con las actualizaciones periódicas) se deposite con un tercero de confianza, lo que permitirá que el código se libere en caso de que la consultora no pueda continuar dando soporte a la Plataforma.

VII. Capacitación para el uso de la Plataforma

La capacitación en el uso de la Plataforma que deberá proveer la consultora se realizará en las oficinas del **Ministerio**, o aquellas que éste facilite o determine y será destinada a:

- **A los usuarios clave**. Orientada a que el **Ministerio**, a través del personal técnico, pueda analizar las brechas de funcionalidad existentes entre el software propuesto y las funcionalidades requeridas detalladas en el **Anexo I: Especificaciones Funcionales y Tecnológicas**.
- **A los administradores y usuarios finales**. Capacitación funcional y técnica, orientada a que el personal del **Ministerio** pueda operar, configurar, modificar y mantener la Plataforma convenientemente.
- **Al personal técnico**. Orientada a las personas a cargo de mantener las integraciones entre sistemas internos y externos.
- **Al personal de Mesa de Ayuda**. Orientada a que el **Ministerio** brinde el soporte funcional y técnico de primer nivel.

VIII. Transferencia Tecnológica

Durante la ejecución de los trabajos de implementación del proyecto, la consultora deberá facilitar al equipo de trabajo del **Ministerio** designado para el seguimiento y conocimiento del mismo, la información y documentación que estos soliciten para disponer del pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de eventuales problemas que puedan plantearse.

IX. Garantía de los Bienes y Servicios

La firma adjudicataria garantizará que todos los bienes y servicios de parametrización, configuración o personalización, suministrados en virtud del contrato que sea conformado estarán libres de defectos atribuibles al diseño, los materiales, o la confección, o a cualquier acto u omisión del oferente que pudiera manifestarse en ocasión del uso normal de los bienes y servicios en las condiciones imperantes en el país.

Los bienes deberán poseer un período de garantía desde la fecha de recepción de los mismos en el lugar de entrega estipulado.

El **Ministerio** notificará de inmediato y por escrito al proveedor cualquier reclamación a que hubiere lugar con arreglo a la garantía y el proveedor reparará o reemplazará los bienes defectuosos en todo o en parte, sin costo para el **Ministerio**, dentro del plazo máximo de **5 (CINCO)** días hábiles de notificada la reclamación.

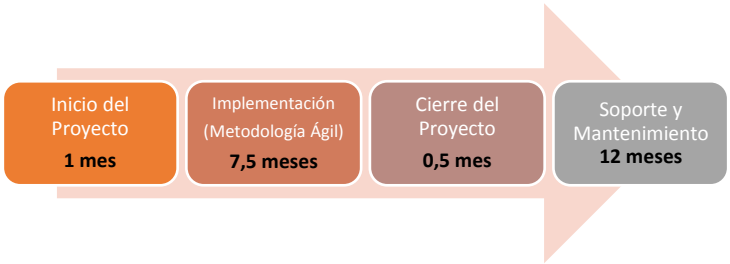
Se entiende por *período de garantía* al espacio de tiempo que va desde la fecha de puesta en producción del proyecto hasta **12 (DOCE)** meses calendario inmediatos, consecutivos y posteriores a la misma.

Durante dicho período, el oferente deberá corregir y enmendar todos los defectos y/o vicios ocultos que pudieran aparecer fruto de la operación en producción de los productos y servicios homologados, diligenciando rápidamente las acciones necesarias para garantizar el correcto funcionamiento de las partes de la solución implementada que no funcionen correctamente o conforme se hayan requerido.

X. Plazos y Entregables

El plazo de tiempo propuesto para el proyecto de implementación no deberá superar los **9 (NUEVE) meses calendarios**.

El plazo de tiempo propuesto para los Servicios de Soporte y Mantenimiento Post-Producción deberá ser de **12 (DOCE) meses consecutivos**, iniciando el mes de la puesta en producción final.



La fecha de inicio efectiva de las tareas del proyecto será como máximo hasta 2 (DOS) semanas posteriores a la fecha de firma del contrato.

A continuación, se listan las tareas mínimas esperadas asociadas al proyecto:

Etapas / sub-etapas		Tareas	Plazos Estimados[5]
Inicio del Proyecto		Conformación del equipo y del Comité Directivo del proyecto.	½ mes
		Disponer la licencia provisional de la Plataforma para el desarrollo del proyecto.	
		Kick-off del proyecto.	
		Capacitación en detalle, orientada al análisis de brechas, de los aspectos funcionales y técnicos de la Plataforma.	½ mes
		Elaboración del documento global de especificaciones de la Plataforma, que incluye: • *Backlog* de todas las especificaciones de alto nivel funcionales, no funcionales y de soporte y mantenimiento que serán implementadas en el proyecto. • Funcionalidad y aspectos técnicos que serán implementados "*as is*" (tales como son provistas por la Plataforma). • Diseño de las implementaciones y sus formas de resolución, parametrizaciones, configuraciones, etc. • Priorización de brechas funcionales y técnicas y las formas de resolución. • Diseño del plan de integración con **FIRMA DIGITAL de AFIP** y el ERP (CRM, Help Desk y Contable), indicando tipo, forma, estrategia de integración y demás especificaciones técnicas.	
		Determinación del número de incrementales (*releases*) para ser implementadas mediante metodología ágil.	
		Elaboración del plan detallado de implementación del proyecto total.	
Implementación Ágil[6] de los incrementales (*releases*)	Análisis y diseño del incremental (*release*)	Selección de especificaciones de la Plataforma para el incremental (*release*) en base al documento global de especificaciones de la Plataforma.	7,5 meses
		Planificación de los *sprints* del incremental (*release*).	
		Análisis de las brechas de los aspectos funcionales y técnicos del incremental (*release*).	
		Diseño de los *sprints* para ajustar las brechas.	
		Elaboración del plan de aceptación de las pruebas del incremental (*release*) **ATP[7]** (*Acceptance Test Plan*).	
	Implementación del incremental (*release*)	Ejecución de los *sprints* y tareas necesarias en un ambiente de desarrollo.	
		Migración al ambiente de prueba.	

[5] *Días y meses calendarios*

[6] *La implementación ágil supone la entrega de módulos con capacidad de conformar una versión incremental del software con características funcionales útiles.*

[7] *Documento que describe el alcance, una aproximación, recursos y agenda de las actividades de pruebas, considerando funcionalidades a ser probadas, las tareas de pruebas, el grado de independencia del que prueba, el entorno de pruebas, el diseño de las técnicas de prueba, los criterios de entradas y salidas que se usarán, la razón de las elecciones y el plan de contingencia para cualquier riesgo que lo requiera.*

Etapas / sub-etapas		Tareas	Plazos Estimados[5]
		Ejecución del plan de aceptación de pruebas del incremental (*release*) (con regresión).	
		Elaboración de la documentación del incremental (*release*).	
		Capacitación del incremental (*release*).	
	Pilotos / Pre-Producción	Planificar el piloto (universo de datos, usuarios y cantidad de incrementales – *releases* involucrados).	
		Ejecución del piloto.	
		En caso de necesidad y en función del resultado de la ejecución de los pilotos: • Readecuar, reconfigurar, re parametrizar, ajustar y/o refinar los incrementales (*releases*). • Ejecutar el plan de aceptación de pruebas (con regresión), homologar configuración, parametrización y desarrollos. • Readecuar la documentación. • Recapacitar. Todo ello realizado en los respectivos entornos que correspondan.	
	Puesta en Producción del Piloto	Migración de datos total inherentes al piloto.	
		Hito de puesta en producción.	
Cierre del Proyecto		Disponer la licencia definitiva de uso de la Plataforma.	½ mes
		Hito de puesta en producción final.	
		Proveer el código fuente (modalidad **ESCROW**).	
		Hito de cierre del proyecto.	
Soporte y Mantenimiento		Provisión de los Servicios de Soporte y Mantenimiento durante todo el proyecto de implementación.	De acuerdo con la duración total del proyecto
		Provisión de los Servicios de Soporte y Mantenimiento desde la puesta en producción final.	12 meses a partir del hito de cierre del proyecto

Los entregables mínimos esperados son:

- **Inicio del Proyecto**
  - Documento con la conformación del equipo de proyecto y el Comité Ejecutivo.
  - Provisión de la licencia provisional de la Plataforma para el desarrollo del proyecto.
  - Reunión de Kick-Off del proyecto.

- Usuarios clave capacitados en los aspectos funcionales y técnicos de la Plataforma, con orientación al análisis de brechas.
- Documento global de especificaciones de la Plataforma.
- Informe con el plan detallado del proyecto de implementación total.

- **Implementación Ágil de los Incrementales (releases)**
  - **Análisis y Diseño del Incremental (*release*)**
    - Documento con las especificaciones de la Plataforma del incremental (*release*).
    - Informe con el plan de trabajo del incremental (*release*) y actividades de los *sprints.*
    - Documento con el análisis, el diseño y la estrategia de implementación de los aspectos funcionales y técnicos del incremental (*sprint*) para cubrir las brechas identificadas en el documento global de especificaciones del software.
    - Documento **ATP** (*Acceptance Test Plan*) del incremental (*release*).
  - **Implementación del Incremental (*release*)**
    - Incremental (*release*) disponible en los ambientes de desarrollo y pruebas.
    - Plan de pruebas ejecutado y homologado en base al documento **ATP** (*Acceptance Test Plan*).
    - Documentación del incremental (*release*).
    - Recursos humanos capacitados en el incremental (*release*).
  - **Pilotos / Pre-Producción**
    - Incrementales (*releases*) disponibles en el ambiente de pre-producción.
    - Datos migrados en el ambiente de pre-producción, aquellos inherentes al piloto.
    - Los siguientes entregables sólo serán obligatorios en caso de que el resultado de la ejecución de los pilotos no se ajuste a lo requerido y serán requeridos por cada comportamiento que no se ajuste a las necesidades prefijadas
      - Nuevos incrementales (*releases*) disponibles en los ambientes de desarrollo y pruebas.
      - Plan de pruebas ejecutado y homologado en base al documento **ATP** (*Acceptance Test Plan*).
      - Documentación.
      - Recursos humanos capacitados.
      - Incrementales (*releases*) disponibles en el ambiente de producción.
    - Piloto homologado y aprobado.
  - **Puesta en Producción del Piloto**
    - Datos totales migrados en el ambiente de producción, aquellos inherentes al piloto.

- **Cierre del Proyecto**
  - Entrega de la licencia definitiva de uso perpetuo de la Plataforma.
  - Hito de puesta en producción final.
  - Depósito del código fuente en modalidad **ESCROW**.
  - Hito de cierre del proyecto

Otros entregables. Durante la implementación del proyecto se deberán cumplir con los siguientes entregables los cuales serán solicitados mediante orden de servicio sin costo adicional.

- Se evaluará con el equipo de proyecto el momento oportuno para realizar estas capacitaciones:
  - Al personal de la Mesa de Ayuda del **Ministerio** para que el **Ministerio** brinde el soporte funcional y técnico de primer nivel.
  - Al personal técnico y a los administradores de la Plataforma de aplicación provisto por la consultora. La capacitación técnica deberá incluir la forma en la cual las integraciones con otros sistemas deben ser mantenidas por el personal técnico del **Ministerio**.
- **Información** y **documentación** que sea requerida en el marco de la "Transferencia Tecnológica del Proyecto".

XI. Anexo I: Especificaciones Funcionales y Tecnológicas

Requerimientos Funcionales

Código	Requerimiento
1.	**Funciones Administrativas**
1.1	**Administración de Entidades Informantes**
1.1.1	Proporcionar a CenFIF la capacidad de registrar y mantener datos relevantes de las entidades informantes, incluidos los datos de identificación, los detalles de contacto, el tipo de entidad, el tipo del reporte y otra información según lo defina CenFIF.
1.1.2	Las entidades informantes registradas estarán habilitadas para tener acceso a la Plataforma. Los usuarios CenFIF tendrán la capacidad de permitir que las entidades informantes utilicen la Plataforma.
1.1.3	Las entidades informantes que operen dentro de un grupo de económico deberán contar con un punto de acceso compartido.
1.1.4	Proporcionar a CenFIF la capacidad de recuperar, ver y editar la información del perfil de las entidades informantes.
1.1.5	Proporcionar a CenFIF la capacidad dar soporte al mantenimiento de los detalles de contacto de la entidad/grupo informante.
1.1.6	Proporcionar a CenFIF la capacidad de registrar las normas NIIF y argentinas relevantes para la entidad informante.
1.1.7	Proporcionar a CenFIF la capacidad de definir y administrar nueva información de perfil de una entidad informante.
1.2	**Administración de Usuarios de CenFIF**

1.2.1	Proporcionar a CenFIF la capacidad de crear y administrar cuentas de usuarios internos con roles, permisos y derechos de acceso para los usuarios designados por CenFIF.
1.2.2	Proporcionar a CenFIF la capacidad de reasignar roles de usuario interno, sujeto a reglas de negocio.
1.2.3	La Plataforma administrará la autenticación de usuarios internos según procedimientos seguros.
1.2.4	Proporcionar a CenFIF la capacidad de configurar permisos por rol para usuarios internos. Por ejemplo, permisos para acceder y utilizar datos, funcionalidades basados en el tipo de datos, en el departamento, en el equipo, etc.
1.2.5	Proporcionar a CenFIF la capacidad de habilitar y deshabilitar manualmente cuentas de usuario internos.
1.2.6	Proporcionar a los usuarios de CenFIF la capacidad de administrar sus credenciales de seguridad. Por ejemplo, cambio la contraseña.
1.3	**Administración de Usuarios de los CPCE**
1.3.1	Proporcionar a CenFIF la capacidad de crear y administrar cuentas de usuario con roles, permisos y derechos de acceso para los usuarios designados por los CPCEs.
1.3.2	Proporcionar a CenFIF la capacidad de reasignar roles de usuario de CPCE, sujeto a reglas de negocio.
1.3.3	Proporcionar a CenFIF la capacidad de monitorear la cantidad de usuarios configurados por un CPCE. Por ejemplo, ver cuántos usuarios ha configurado un CPCE para limitarlos si se alcanza un límite determinado.
1.3.4	Autenticar y permitir el acceso a la Plataforma a los usuarios de los CPCE mediante credenciales de FIRMA DIGITAL de AFIP.
1.3.5	Proporcionar a CenFIF la capacidad de habilitar y deshabilitar manualmente cuentas de usuarios de CPCEs. Por ejemplo, es posible que CenFIF desee desactivar usuarios que no hayan accedido al sistema en los últimos 6 meses.
1.4	**Administración de Usuario de las Entidades Informantes**
1.4.1	Proporcionar a CenFIF la capacidad de crear y administrar cuentas de usuario con roles, permisos y derechos de acceso para los usuarios designados por las entidades informantes. ▪ Proporcionar a los usuarios de CenFIF la capacidad de administrar los datos de contacto del contacto principal de una entidad informante. ▪ Proporcionar al usuario principal de la entidad informante la capacidad de administrar el resto de los datos de contacto de sus usuarios.
1.4.2	Proporcionar CenFIF la capacidad de reasignar roles de usuario externos, sujeto a reglas de negocio.
1.4.3	Proporcionar a CenFIF la capacidad de definir y administrar grupos de entidades informantes. Por ejemplo, permitir que un único usuario de una entidad informante realice acciones en la Plataforma para varias entidades informantes del mismo grupo sin tener que iniciar sesión varias veces.
1.4.4	Autenticar y permitir el acceso a la Plataforma a los usuarios externos mediante credenciales de FIRMA DIGITAL de AFIP.
1.4.5	Proporcionar a CenFIF la capacidad de habilitar y deshabilitar manualmente cuentas de usuarios externos. Por ejemplo, es posible que CenFIF desee desactivar usuarios que no hayan accedido al sistema en los últimos 6 meses.
1.5	**Administración de Taxonomías XBRL**
1.5.1	Proporcionar a CenFIF la capacidad de gestionar diferentes taxonomías XBRL, según el tipo de entidad informante y la normativa vigente.
1.5.2	Proporcionar a CenFIF la capacidad de agregar, mantener y administrar versiones de todas las plantillas y taxonomías de envío de datos dentro la Plataforma, incluidas las reglas y

	metadatos relacionados, como también los intervalos de fechas aplicables, el calendario de reportes, etc.
1.5.3	Proporcionar a CenFIF la capacidad de administrar versiones de plantillas de reporte estructurados y no estructurados según defina CenFIF.
1.6	**Administración de Perfiles de Reporte y Calendarios**
1.6.1	Proporcionar CenFIF la capacidad de definir y administrar diferentes perfiles de reporte que se asignarán a cada entidad informante. El perfil de reporte se asociará a uno o varios requisitos de reporte que deberán cumplir las entidades informantes según su perfil.
1.6.2	Proporcionar a CenFIF la capacidad de definir y gestionar diferentes tipos de requisitos de reporte, indicando la taxonomía de reporte que se presentará, el calendario de presentación (frecuencias y vencimientos) y las firmas digitales de los preparadores, auditores y CPCE que requerirán confirmar los datos presentados.
1.6.3	Proporcionar a CenFIF la capacidad de solicitar cambios en los requisitos de reporte para una entidad informante. Por ejemplo, solicitar un requisito de reporte adicional debido a un evento significativo.
1.6.4	Para cada plantilla de reporte en un calendario, la Plataforma determinará automáticamente la fecha límite de envío en función de los datos del perfil de la entidad informante. Por ejemplo, para el reporte anual se requerían un número específico de semanas después de la fecha de cierre de los estados contables.
1.6.5	Proporcionar a CenFIF la capacidad de recibir extensiones a la fecha de reporte y el motivo de la extensión, si se proporciona.
1.6.6	Proporcionar a las entidades informantes la capacidad de ver sus requisitos y calendario de reportes.
1.6.7	Proporcionar a CenFIF la capacidad de monitorear el cumplimiento de los requisitos de reporte por parte de las entidades informantes y establecer alertas en función de la actividad de monitoreo.
1.6.8	Proporcionar a CenFIF la capacidad de generar alertas automáticas y notificaciones a las entidades informantes cuando los calendarios de los requisitos de reporte estén vencidos.
2.	**Administración del Proceso de Intercambio de Información**
2.1	**Autenticación de Mensajes**
2.1.1	Todos los mensajes enviados por usuarios externos y de CPCEs deberán ser autenticados basados en la FIRMA DIGITAL de AFIP.
2.2	**Envío de Documentos Instancia en XBRL**
2.2.1	El envío de documentos instancia a la Plataforma se realizará de dos maneras, ya sea a través de un “servicio sistema a sistema” o a través de un “portal de carga de documentos”. CenFIF podrá brindar soporte a aquellas entidades informantes que deseen integrar sus sistemas de back-office con la Plataforma, para poder procesar los envíos directamente sin necesidad de acceder manualmente a una interfaz de usuario basada en la web.
2.2.2	Proporcionar a CenFIF la capacidad de definir y configurar las reglas de intercambio para los documentos instancia en XBRL que deberán enviar las entidades informantes. Las reglas de intercambio incluirán opciones tales como: ▪ Permitir o rechazar el envío de documentos instancia fuera del calendario de reporte. ▪ Definir un período de tiempo durante el cual el remitente puede cancelar un envío. ▪ Suspender temporalmente la recepción de documentos instancia.
2.2.3	Proporcionar a los usuarios autorizados de las entidades informantes la capacidad de enviar documentos instancia a la Plataforma, siguiendo las reglas de intercambio definidas por CenFIF. El usuario deberá especificar el requisito de reporte y el período correspondiente al documento instancia.
2.2.4	Proporcionar a los usuarios autorizados de las entidades informantes la capacidad de cancelar un documento instancia enviado previamente dentro de un período de tiempo definido por CenFIF.

2.2.5	Proporcionar a los usuarios autorizados de las entidades informantes la capacidad de volver a enviar los datos informados previamente en cualquier momento y para cualquier período histórico. Por ejemplo, corregir datos.
2.2.6	La Plataforma tendrá la capacidad de capturar la fecha de presentación / reenvío.
2.2.7	La nueva presentación deberá especificar el requisito de reporte, el período a corregir y los motivos de la modificación. El motivo del reenvío puede ser una lista predefinida y/o un formato libre.
2.2.8	Proporcionar a CenFIF la capacidad de opcionalmente revisar los reenvíos y aprobar o rechazar el nuevo envío, manualmente o sujeto a reglas de negocio. En caso de no ser puesto en espera o rechazado, el nuevo documento instancia será validado y sustituirá los datos informados anteriormente. Los nuevos datos informados se marcarán como reenvíos y el documento de instancia enviado anteriormente se almacenará y será accesible en la Plataforma.
2.2.9	Proporcionar a los usuarios autorizados de las entidades informantes la capacidad de consultar la lista y el estado de los documentos instancia enviados.
2.2.10	Proporcionar a los usuarios de CenFIF, de CPCEs y externos la capacidad de intercambiar mensajes de información con archivos adjuntos estructurados o no estructurados.
2.2.11	La Plataforma tendrá la capacidad de recibir envíos de datos en los siguientes formatos electrónicos: Excel, CSV y XML. También deberá proporcionar una página Web para que la entidad informante cargue los datos directamente.
2.2.12	La Plataforma tendrá la capacidad de recibir datos no estructurados de entidades informantes para el almacenamiento de documentos. Por ejemplo, copia de actas de directorio.
2.2.13	Proporcionar a los usuarios de las entidades informantes la capacidad de cargar archivos individualmente.
2.2.14	Proporcionar a los usuarios de las entidades informantes la capacidad de cancelar la carga de un archivo o varios archivos después de que haya comenzado.
2.2.15	Proporcionar a CenFIF la capacidad de almacenar y ver cualquier envío válido de una entidad informante (envíos actuales y anteriores). Por ejemplo, para uso en análisis de tendencias.
2.2.16	Proporcionar a los usuarios de las entidades informantes la capacidad de cargar varios archivos a la vez.
2.2.17	Proporcionar a los usuarios de las entidades informantes un indicador de progreso al cargar un archivo(s). Por ejemplo, % barra de progreso.
2.2.18	Proporcionar a los usuarios de las entidades informantes la capacidad de asociar información estructurada y/o metadatos a los datos que se envían.
2.2.19	Proporcionar a los usuarios de las entidades informantes la capacidad de marcar una plantilla de reporte como “No Reportada”.
2.2.20	Proporcionar a CenFIF la capacidad de ver cualquier envío válido de una entidad informante (envíos actuales y anteriores) y de cargar documentos de trabajo para almacenar junto con los datos archivados. Por ejemplo, para que los usuarios vean lo que otros colegas analizaron o informaron.
2.3	**Proceso de Envío y Validación**
2.3.1	La Plataforma realizará automáticamente la validación de las presentaciones, en función del tipo de requisito de reporte asociado a la presentación. En particular, el sistema realizará las siguientes comprobaciones: ▪ Se autenticará la firma del remitente, del auditor y del CPCE. ▪ El remitente es un usuario autorizado de la entidad informante para realizar el envío. ▪ El envío corresponde al requisito y al período de reporte de la entidad informante.

	▪ El envío incluye las firmas requeridas para el tipo de requisito de reporte, confirmando los datos financieros y el informe del auditor incluidos en el documento instancia. ▪ El envío incluye un documento instancia correspondiente a la versión de la taxonomía especificada para el requisito de reporte. ▪ El informe del auditor corresponde a los estados contables presentados.
2.3.2	La Plataforma notificará a la entidad informante con el resultado de la validación de la presentación y, en caso de rechazo, indicará los motivos del rechazo.
2.3.3	La Plataforma determinará automáticamente cómo procesar los datos presentados basándose en un conjunto de criterios y reglas predefinidas, es decir, cómo y dónde almacenar y dónde encaminar los datos dentro de la Plataforma. Por ejemplo, los criterios y las reglas de validación a utilizar pueden basarse en el formato de archivo, los metadatos, los datos del perfil de la entidad informante, etc.
2.3.4	La Plataforma recibirá y almacenará todos los datos válidos presentados. Por ejemplo, si una entidad informante realiza un envío de datos válido y luego, en un momento posterior del mismo período de reporte, realiza un reenvío que también es válido, entonces ambos envíos deberán almacenarse.
2.3.5	La Plataforma restringirá a los usuarios de CenFIF de modificar los datos recibidos en de la Plataforma por parte de terceros. Por ejemplo, datos enviados por entidades informantes o fuentes de datos de terceros. Nota: los usuarios de CenFIF deberán poder modificar ciertos datos ingresados manualmente, como ser los datos adjuntos a los datos recibidos.
2.3.6	La Plataforma deberá priorizar el procesamiento de los envíos de ciertas entidades informantes sobre otras basadas en criterios o reglas de negocio. Por ejemplo, por categoría, por tipo de entidad informante, etc.
2.3.7	La Plataforma almacenará los datos no válidos recibidos, hasta que puedan ser reemplazados automáticamente por un conjunto válido de datos, ya sea a través de un reenvío o una nueva ejecución de las reglas de validación por parte de usuarios de CenFIF. Por ejemplo, los datos recibidos no necesitan pasar la validación para ser almacenados, para permitir que los usuarios de CenFIF accedan a los datos en circunstancias excepcionales. Además, la experiencia sugiere que algunas reglas de validación serán incorrectas y requerirán la corrección por parte de un usuario de CenFIF. Al volver a ejecutar las reglas corregidas, debería ser posible volver a validar los datos sin necesidad de volver a enviarlos.
2.3.8	La Plataforma determinará automáticamente la clasificación de seguridad de los datos de un archivo según reglas de negocio predefinidas. Por ejemplo, se puede asignar como “confidencial” por defecto a un determinado conjunto de datos que probablemente contengan datos sensibles de mercado (utilizando metadatos) con acceso predeterminado a usuarios específicos de CenFIF.
2.3.9	Proporcionar a CenFIF la capacidad de definir y configurar las reglas del sistema que determinan dónde almacenar y como acceder a los archivos, el nombre y cómo clasificarlos. Por ejemplo, si CenFIF cambia su estructura de archivos, querrá actualizar las reglas para reflejar los cambios.
2.3.10	La Plataforma realizará el seguimiento automáticamente el estado de un envío a través de las varias etapas del proceso. Por ejemplo, presentado, validado, comprobación de verosimilitud, exportado, etc. Esto posibilitará a CenFIF saber hasta qué punto se han procesado los datos en caso de que una entidad informante vuelva a enviar los datos.
2.3.11	Proporcionar a CenFIF la capacidad de agregar datos adicionales a un elemento de datos y ver lo que se ha agregado. Por ejemplo, para investigación de verosimilitud.
2.4	**Administración y Comprobación de Reglas de Verosimilitud**
2.4.1	Proporcionar a CenFIF la capacidad de definir y configurar reglas de verosimilitud (además de las reglas de validación definidas en la taxonomía) para los datos definidos por CenFIF. Las comprobaciones de verosimilitud pueden incluir comprobar si un elemento de datos es

	inusualmente grande o pequeño, comprobar que un conjunto de datos se encuentra dentro de un rango de valores predefinido, etc.
2.4.2	CenFIF podrá acceder y utilizar datos de fuentes de terceros dentro de la Plataforma para respaldar la actividad de procesamiento, como la comprobación de verosimilitud. Los datos pueden estar disponibles a través de carga manual, carga por lotes o integración. Los ejemplos de tipos de datos incluyen tipo de cambio, listas de datos de referencia y datos de mercado.
2.4.3	Proporcionar a CenFIF la capacidad de configurar y administrar grupos de entidades informantes para respaldar las reglas de verosimilitud. Por ejemplo, la capacidad de configurar grupos de pares para ejecutar comprobaciones de verosimilitud específicas por sector o grupo de pares o comprobaciones que tienen variables específicas de un sector o grupo de pares.
2.4.4	Proporcionar a CenFIF la capacidad de activar y desactivar individualmente las reglas de verosimilitud, es decir, para todas o algunas entidades informantes, o todas las reglas o algunas para todas las entidades informantes.
2.4.5	Proporcionar a CenFIF la capacidad de definir qué reglas de verosimilitud deberán activarse automáticamente y cuáles de forma manual.
2.4.6	Proporcionar a CenFIF la capacidad de ejecutar de forma manual o automática las verificaciones de verosimilitud contra los datos enviados.
2.4.7	Proporcionar a los usuarios relevantes de CenFIF la capacidad de ver el resultado de la comprobación de verosimilitud. Por ejemplo, resultado rojo, amarillo o verde.
2.4.8	Proporcionar a CenFIF la capacidad de definir y configurar alertas y notificaciones según el resultado de la aplicación de las reglas de verosimilitud.
2.5	**Validación de Documentos Instancia**
2.5.1	Proporcionar a CenFIF la capacidad de definir y configurar diferentes procedimientos estandarizados para validar documentos instancia, según el perfil de la entidad informante y el tipo de requisito de reporte.
2.5.2	Proporcionar a CenFIF la capacidad de configurar reglas de validación definidas internamente.
2.5.3	Proporcionar a CenFIF la capacidad de controlar la versión de todas las reglas de validación, con la capacidad de seleccionar qué reglas aplicar. Por ejemplo, activar y desactivar reglas de validación individualmente o en base a entidades informantes en particular.
2.5.4	Proporcionar a CenFIF la capacidad de comprobar los cambios en la validación antes de aplicarlos en producción.
2.5.5	La Plataforma podrá determinar automáticamente qué reglas de validación deberán aplicarse a un reenvío de datos. Por ejemplo, es posible que deba aplicarse un conjunto anterior de reglas de validación a los datos enviados nuevamente, y que las reglas de validación actuales se apliquen solo a las nuevas presentaciones.
2.5.6	La configuración deberá permitir definir si los documentos se validarán automáticamente en la recepción o si se almacenarán temporalmente antes de la validación. La configuración también debería permitir definir si la validación de documentos instancia almacenados temporalmente se iniciará de forma manual o automática, en función de parámetros tales como el volumen de documentos almacenados, ventanas de tiempo predefinidas, etc.
2.5.7	Basado en el procedimiento de validación asociado al envío, la Plataforma realizará automáticamente la validación del documento instancia en XBRL , según las reglas de validación especificadas en cada taxonomía.
2.5.8	La Plataforma informará a las entidades informantes sobre el estado y el resultado del proceso de validación. En caso de no validación, la Plataforma enviará a la entidad informante una notificación que indique los motivos del rechazo.
2.5.9	La Plataforma permitirá “straight-through processing” (STP) en caso de documentos instancia sin errores.

	La Plataforma procesara automáticamente los datos a menos que tenga un resultado de validación “fallido” o un resultado de comprobación de verosimilitud especifico.
2.5.10	Proporcionar a CenFIF la capacidad de procesar manualmente los datos en casos excepcionales. Por ejemplo, incluso si los criterios de calidad predefinidos no se han cumplido.
2.6	**Monitoreo de los Envíos**
2.6.1	Proporcionar a CenFIF la capacidad de monitorear con un tablero de control el estado de las presentaciones actuales y anteriores de las entidades informantes. El tablero proporcionará información online respecto a: ▪ Número de envíos recibidos, validados y rechazados. ▪ Número de documentos instancia presentados, validados y rechazados. ▪ Nivel de cumplimiento de cada requisito de reporte por período, indicando los documentos instancia, validados, rechazados y vencidos. El tablero de control permitirá definir el período de reporte y desagregar la información según varios criterios, como el perfil de la entidad informante, el tipo de requisito de reporte, el período, el tipo de rechazo, etc.
2.6.2	Proporcionar a CenFIF la capacidad de buscar, filtrar, seleccionar, ver e imprimir los datos enviados por las entidades informantes en un formato legible. Por ejemplo, Excel, CSV, XML y PDF.
2.6.3	Proporcionar a CenFIF la capacidad de identificar la versión más reciente del mismo elemento de datos que sean parte de múltiples envíos por parte de una entidad informante.
2.6.4	Proporcionar a CenFIF la capacidad de profundizar en los datos hasta su nivel de granularidad más bajo. Por ejemplo, ver todos los componentes de las reglas de validación o verosimilitud.
3.	**Extracción y Almacenamiento de Datos**
3.1	La Plataforma extraerá y almacenará automáticamente los datos de los documentos instancia, una vez que se complete la validación. Para este propósito, la Plataforma incluirá una base de datos relacional para almacenar los datos extraídos de los documentos instancia.
3.2	La base de datos relacional mantendrá series históricas de datos informados con cálculos de agregados, totales, tendencias y otras operaciones matemáticas basadas en parámetros.
3.3	Proporcionar a CenFIF la capacidad de definir informes analíticos estandarizados basados en datos históricos, a los que puedan acceder usuarios internos y externos.
3.4	La Plataforma almacenará los documentos instancia validados en XBRL .
4.	
4.1	Proporcionar a CenFIF la capacidad de configurar y enviar notificaciones estandarizadas y personalizadas basadas en una serie de eventos a lo largo del ciclo de administración de datos.
4.2	Proporcionar a CenFIF la capacidad de definir notificaciones con: ▪ Contenido fijo. ▪ Combinación de contenido fijo y variable. – Manualmente poblada. – Auto poblada.
4.3	Proporcionar a CenFIF la capacidad de revisar, enmendar, suprimir y/o liberar notificaciones a los usuarios de los CPCEs y externos. Por ejemplo, las entidades informantes recibirán notificaciones sobre diferentes eventos relacionados con el envío y la verificación de datos.
4.4	Cuando se envían notificaciones a usuarios externos, se deberá mantener la seguridad adecuada. Por ejemplo, la información confidencial no deberá enviarse por correo electrónico y, en su lugar, se deberá solicitar al usuario que inicie sesión en el sistema para ver la información confidencial.

4.5	La Plataforma enviará automáticamente notificaciones para informar a los usuarios de CenFIF cuando se requiera la acción del usuario dentro del sistema.
4.6	La Plataforma enviará automáticamente notificaciones cuando se requiera la acción de un usuario del CPCE o externo.
4.7	La Plataforma enviará automáticamente notificaciones después de un período de tiempo predefinido basado en reglas.
4.8	La Plataforma enviará automáticamente notificaciones basadas en eventos del sistema.
4.9	Proporcionar a CenFIF la capacidad de activar y desactivar las notificaciones por tipo y/o por entidad informante.
4.10	Proporcionar a los usuarios de las entidades de informes la capacidad de adjuntar un archivo con su respuesta a una validación y/o notificación de verosimilitud. Por ejemplo, el usuario responde a una consulta de verosimilitud con un mensaje explicativo y una hoja de cálculo adjunta. Esto es para asegurar que la hoja de cálculo se mantenga junto con el mensaje.
4.11	La Plataforma registrará automáticamente la razón del resultado de verosimilitud utilizando la última respuesta proporcionada por un usuario externo, es decir, sin que el usuario de CenFIF tenga que cortar y pegar manualmente la información de respuesta del usuario externo en el sistema.
4.12	Proporcionar a los usuarios externos la capacidad de consultar el estado de un envío y recibir notificaciones del estado o eventos.
5.	**Rol como Operador Central**
5.1	Proporcionar a CenFIF la capacidad de extraer automáticamente los datos de los reportes almacenados y enviarlos al software de business intelligence.
5.2	Proporcionar a CenFIF la capacidad de utilizar datos estructurados con fines analíticos, sujeto a que los datos se reciban en un formato estándar. Por ejemplo, formato Excel, XBRL, Inline XBRL, CSV, etc.
5.3	La Plataforma tendrá la capacidad de interactuar con aplicaciones externas, como ser fuentes de datos de referencia, ERP, etc.
6.	**Divulgación de Información**
6.1	**Acceso Público a la Información**
6.1.1	Proporcionar a usuarios públicos la capacidad de buscar, seleccionar y ver documentos instancia de entidades informantes en un formato legible (Web, EXCEL y PDF) o descargar documentos instancia en XBRL. Los criterios de búsqueda incluirán el identificador, el nombre de la entidad informante, el requisito de reporte, el período de reporte, etc.
6.1.2	Proporcionar a CenFIF la capacidad de asociar automáticamente un indicador de divulgación (abierto, restringido) a los documentos instancia según el estado y el resultado de la validación.
6.1.3	Proporcionar a CenFIF la capacidad seleccionar y asociar manualmente un indicador de divulgación (abierto, restringido) a un conjunto particular de documentos instancia y/o elementos, en función de criterios como la entidad informante, los requisitos de reporte, el período de reporte, etc.
6.1.4	Los usuarios públicos estarán autorizados a acceder solo a aquellos documentos instancia y/o elementos marcados como abiertos.
6.2	
6.2.1	Proporcionar a CenFIF la capacidad de preparar, extraer y transferir datos a terceros, incluido la posibilidad de definir, revisar y filtrar conjunto de datos.
6.2.2	Proporcionar a CenFIF la capacidad de configurar conjuntos de datos para que se compartan automáticamente con terceros.
6.2.3	La Plataforma enviará o pondrá a disposición automáticamente datos a terceros sujetos a la configuración definida por CenFIF.
6.2.4	Proporcionar a CenFIF la capacidad de extraer manualmente los datos necesarios para enviar a terceros.

6.2.5	Proporcionar a CenFIF la capacidad de extraer datos del sistema en formatos estándar. Por ejemplo, Excel, CSV, XML, XBRL, Inline XBRL, etc.
6.2.6	Proporcionar a CenFIF la capacidad de detener manualmente que los datos se envíen automáticamente a un tercero.
6.2.7	Proporcionar a CenFIF la capacidad de enviar datos manualmente a un tercero.
6.2.8	Proporcionar a CenFIF la capacidad de revisar datos antes de enviarlos a terceros.
7.	**Reportes Operativos**
7.1	Proporcionar a CenFIF la capacidad generar informes que detallen la actividad que se está realizando y el estado de la información que se encuentre procesando en toda la Plataforma. Por ejemplo, distinguir datos válidos e inválidos, por estado de envío, estado de entidades informantes, etc.
8.	**Servicios de Ayuda y Soporte al Usuario**
8.1	Proporcionar a los usuarios de CenFIF soporte para el uso efectivo de la Plataforma. Por ejemplo, guías de usuario, webinars, etc.
8.2	Proporcionar a los usuarios de CenFIF los servicios de *Help Desk* en pantalla.
8.2	Proporcionar a CenFIF la capacidad de emular entidades informantes para ayudar a proporcionar soporte técnico y de usuario a las entidades informantes.

Requerimientos No Funcionales

Código	Requerimiento
1.	**Datos**
1.1	**Exactitud** Todas las notificaciones, solicitudes de datos y datos recopilados se presentará con precisión a los usuarios apropiados de la Plataforma (ya sea usuario de CenFIF, de entidad informante, de CPCE o usuario externo).
1.2	**Archivo** La Plataforma deberá proporcionar a los usuarios de CenFIF la capacidad de definir políticas de archivo y recuperación de datos para diferentes plantillas de reportes y tipos de envío. Por ejemplo, que archive todas las plantillas de reporte después de 10 años, etc.
1.3	**Integridad** La integridad de los datos deberá mantenerse desde el punto de recepción y durante todo su procesamiento, manejo y uso de dichos datos.
1.4	**Metadatos** Los metadatos deberán estar asociados a un archivo en el momento de la carga en la Plataforma. ¿Dónde y cómo se almacenan estos metadatos? ¿Es posible configurar qué metadatos estén asociados?
1.5	**Almacenamiento** La Plataforma deberá poder almacenar los datos en el formato original que se ha enviado.
1.6	**Recuperación** Proporcionar a CenFIF la capacidad de poder recuperar datos archivados cuando sea necesario. Por ejemplo, archivos de datos sin procesar junto con versiones relevantes de las taxonomías y la documentación de respaldo.
2.	**Desarrollo y Mantenimiento**
2.1	**Cambios**

	Cualquier cambio en la Plataforma deberá poder ser empaquetado e implementado de forma incremental y automática.
2.2	**Desarrollo** El acceso de solo lectura al modelo de datos subyacente de la Plataforma deberá estar soportado y documentado para permitir que CenFIF cree sus propios informes o utilice los datos de otros sistemas.
2.3	**Entornos**
2.3.1	CenFIF necesitará entornos diferenciados para soportar: ▪ Producción. – Entorno go live. ▪ Pre-producción. ▪ Pruebas de aceptación de usuario. ▪ Pruebas de integración del sistema. – Entorno principal de prueba del sistema. ▪ Desarrollo. ▪ Entrenamiento. Los usuarios deberán tener diferentes credenciales de inicio de sesión para iniciar sesión en diferentes entornos.
2.3.2	Para admitir la integración de "sistema a sistema / B2B", la Plataforma deberá ser compatible con dos tipos de entornos de prueba externos para que proveedores de software / terceros puedan realizar pruebas: ▪ Una versión de la Plataforma de producción actual. ▪ Una versión que contiene nuevos cambios en la Plataforma.
2.3.3	Los entornos de prueba deberán ser claramente distinguibles para que el usuario sepa a qué versión está accediendo.
2.4	**Extensibilidad**
2.4.1	La Plataforma deberá poder ampliarse para funciones nuevas sin tener que reconstruirla completamente.
2.5	**Comprobabilidad**
2.5.1	La Plataforma deberá ser fácilmente comprobable mediante herramientas de prueba automatizadas y pruebas de regresión. ▪ ¿Las pruebas automatizadas están integradas en el proceso de desarrollo y mantenimiento? ▪ ¿Utiliza herramientas de prueba automatizadas para nuevas funciones y pruebas de regresión? ▪ ¿Se proporcionarán estas herramientas a CenFIF? ▪ ¿Utiliza alguna herramienta de gestión de pruebas? ▪ ¿Cómo se realizan las pruebas de regresión? ▪ ¿Qué elementos de prueba de regresión pretende producir como parte del proyecto y si estarán disponibles para CenFIF (posterior a la implementación)?
3.	**Recuperación de Desastres**
3.1	**Recuperación de la Plataforma** Si existe sospecha de corrupción de datos en la Plataforma en el caso de un ciberataque u otro evento importante, deberá ser posible recuperarla en un punto donde se sabe que los datos son correctos.
3.2	**Pruebas** La Plataforma deberá ser probada para recuperación de desastres de acuerdo con las políticas estándar del **Ministerio** y del **ONTI**.
4.	**Eficiencia**
4.1	**Datos de Rendimiento** Deberá ser posible recopilar y ver los datos de rendimiento de la Plataforma a medida que se procesan los datos. Por ejemplo, las siguientes áreas deben ser medibles:

	▪ Subida de datos a interfaz externa. ▪ Transferencia de datos desde la interfaz externa al repositorio de datos. ▪ Tiempo para procesar las reglas de validación y verosimilitud.
4.2	**Tiempo de Respuesta de Validación** La Plataforma deberá admitir reportes con un tamaño de archivo de instancia de hasta 50 MB. La Plataforma deberá admitir la recopilación, la validación y el procesamiento de [indique la cifra según el volumen máximo de instancias por día, inicialmente 30.000] en un plazo máximo de 24 horas.
4.3	**Tiempo de Respuesta de la Aplicación Web** Los objetivos de rendimiento deben estar en línea con el resto de las aplicaciones del **Ministerio**. Por ejemplo, excluyendo la red de la entidad informante y el rendimiento del navegador, etc., tiempo promedio para cargar una interfaz de usuario simple en la pantalla en menos de 1 segundo para el 90% de la carga de página, 3 segundos para el 90% de la carga de página para páginas de pantalla media/compleja/baja intensidad de datos, 7 segundos para el 90% para páginas de alta intensidad de datos.
5.	**Legal**
5.1	**Cookies** Las cookies persistentes y de sesión pueden ser necesarias para utilizar la Plataforma. Se deberá solicitar el consentimiento cuando lo exija la ley.
5.2	**Reglamento** La Plataforma deberá cumplir con toda la legislación aplicable en todas las jurisdicciones relevantes, incluidas, entre otras: ▪ Derechos de autor. ▪ Protección de datos. ▪ Otras regulaciones.
6.	**Fiabilidad**
6.1	**Disponibilidad y Horas de Servicio** La Plataforma debe estar completamente operativa el 99.0% del tiempo.
6.2	**Copias de Seguridad** ▪ Las copias de seguridad de la base de datos deberán realizarse a intervalos regulares. ▪ También deberá ser posible elegir un punto en el tiempo para recuperarse. ▪ La Plataforma proporcionará o admitirá la función de copia de seguridad / restauración automatizada. ▪ CenFIF podrá controlar la frecuencia y el tiempo de las copias de seguridad.
6.3	**Recuperación** La Plataforma deberá poder integrar los datos recibidos (a través de medios alternativos durante un período de recuperación) mientras no esté disponible.
6.4	**Estabilidad** En el caso de una falla de sistema, si la Plataforma está en medio de un procesamiento, podrá reiniciarse desde la última transacción confirmada.
7.	**Requerimientos de Seguridad**
7.1	**Acceso** La Plataforma debe usar el acceso basado en roles para controlar qué características de la Plataforma y qué datos pueden usar los usuarios según el principio de privilegio mínimo.
7.2	**Registro para Auditoría**
7.2.1	La Plataforma llevará un registro para auditoría de toda la actividad del sistema. Por ejemplo, registros de autenticación de inicio de sesión/seguridad, actividad de usuario externo, actividad de programación, registros de carga de archivos, actividad de usuario interno, datos de terceros enviados, actividad de validación, actividad de verosimilitud, actividad de notificación, actividad de reportes, actividad de acceso a datos, cambios de datos, cambios en las reglas, etc.

7.2.2	El registro para auditoría debe contener como mínimo: ▪ El usuario que ejecuta la acción. ▪ La fecha y hora del evento. ▪ La acción que se está ejecutando. ▪ Informes de seguridad / inicio de sesión (incluidos inicios de sesión fallidos)
7.2.3	La Plataforma mantendrá un registro para auditoría para cada conjunto de datos enviados a un tercero, incluidos, entre otros, los datos que se enviaron y cuándo. Por ejemplo, ver un registro línea por línea de las presentaciones enviadas y poder acceder al contenido real enviado.
7.2.4	La Plataforma auditará todas las notificaciones enviadas tanto a las entidades informantes y CPCEs como a nivel interno.
7.2.5	Proporcionar a CenFIF la capacidad de restringir el acceso a todos los registros de auditoría de actividad del usuario y del sistema, así como la capacidad de buscar, filtrar y exportar estos datos a ciertos roles del sistema.
7.3	**Autenticación**
7.3.1	▪ Interno: según procedimientos seguros. ▪ Externo: mediante FIRMA DIGITAL de AFIP.
7.4	**Cifrado**
7.4.1	El sistema debe utilizar estándares de cifrado según lo definido / aprobado por el **Ministerio** y el **ONTI**.
7.4.2	La solución debe garantizar que los datos estén protegidos cuando se transmiten entre CenFIF y terceros.
7.5	**Fingerprinting**
7.5.1	▪ Los archivos deben contener fingerprints utilizando un algoritmo apropiado. ▪ El fingerprint debe ocurrir en la carga del archivo. ▪ El fingerprint debe ocurrir en la recepción del archivo para verificar que coincida con el fingerprint de carga.
7.6	**Seguimiento de Incidencias y Respuesta**
7.6.1	La Plataforma deberá ser monitoreada para detectar incidentes de seguridad, recopilar registros o auditar información sobre incidentes de seguridad. Por ejemplo, violaciones de la política de control de acceso, cambios de datos estáticos, agregar, eliminar y cambiar usuarios, seguimiento de actividades, manipulación de archivos del sistema, etc. ▪ ¿Qué información se registrará? ▪ ¿En qué formato se grabará? ▪ ¿Dónde se registrará? ▪ ¿Cómo se accederá a los registros?
7.6.2	Los eventos deberán integrarse en un proceso de respuesta de incidentes, donde todos los incidentes significativos son alertados, gestionados e informados.
7.7	**Malware** Los archivos entrantes deberán ser revisados en busca de malware en la DMZ antes de ingresar a la Plataforma y a la red interna de CenFIF.
7.8	**Contraseñas** ▪ La Plataforma no deberá transmitir contraseñas a través de una red externa en texto claro. ▪ La Plataforma no deberá presentar contraseñas desenmascaradas. ▪ La Plataforma no deberá almacenar contraseñas en texto claro y deberá almacenarse como un “salted hash”. ▪ La Plataforma deberá transferir contraseñas a través de una conexión segura. ▪ La Plataforma deberá imponer formatos de contraseña segura.
7.9	**Preguntas y Respuestas de Seguridad** Cualquier conjunto de preguntas de seguridad para las entidades informantes o CPCEs y las respuestas relacionadas deberán seguir las mejores prácticas de la industria.

7.10	**Tiempo de Espera de Inactividad de Sesión** Se deberá establecer y configurar un valor de tiempo de espera automático para inactividad dentro del sistema. Por ejemplo, 30 minutos.
7.11	**Terminación de Sesión** Cuando se cierre la ventana o cuando se desconecte, o si la Plataforma terminase inesperadamente, la sesión deberá finalizar. La Plataforma deberá utilizar cookies basadas en sesión.
7.12	**Cuentas de Usuario**
7.12.1	La administración de cuentas de usuario internas deberá administrada por un equipo de CenFIF.
7.12.2	Las cuentas de usuario inactivas deberán revisarse y bloquearse después de 6 meses.
7.13	**Servicio y Monitoreo del Sistema**
7.13.1	La Plataforma deberá ser monitoreada.
7.13.2	La Plataforma deberá ser capaz de identificar cuántos usuarios hay y quién está conectado/usando el sistema, su dirección y hora de IP, etc.
8.	**Usabilidad**
8.1	**Accesibilidad** El sistema debe mantenerse al día con las mejores prácticas y estándares internacionales. Por ejemplo: ▪ La Plataforma deberá cumplir con los puntos de verificación de Prioridad 1 y 2 para lograr el cumplimiento del Nivel AA como se especifica en los lineamientos WCAG 2.0. ▪ La Plataforma deberá cumplir con el nivel AA. Esto debe ser probado y certificado de forma independiente. ▪ La Plataforma deberá funcionar con lectores de pantalla asistida para admitir entidades informantes con usuarios que tienen discapacidades visuales o que tienen menos capacidad para usar sitios web sin el uso de tecnologías de asistencia. ▪ La Plataforma deberá admitir a los usuarios que pueden no ser capaces de usar un mouse y necesitarán usar el sistema exclusivamente a través de un teclado.
8.2	**Compatibilidad de los Navegadores**
8.2.1	La Plataforma deberá ser compatible con el siguiente navegador web: ▪ Mozilla Firefox - tres últimas versiones ▪ Google Chrome - tres últimas versiones ▪ Safari - tres últimas versiones ▪ Microsoft Edge - tres últimas versiones
8.2.2	Las pruebas de compatibilidad del navegador se llevarán a cabo en todos los navegadores especificados en 8.2.1.
8.3	**Calendario** Deberá ser posible establecer días festivos, días no laborables, etc. que puedan ser utilizados por otra funcionalidad del sistema. Esto debería estar disponible en cada entorno.
8.4	**Mensajes de Error**
8.4.1	La Plataforma deberá mostrar mensajes de error a los usuarios finales en español e inglés significativo y sencillo, según la configuración del usuario.
8.4.2	Los mensajes de error del sistema se deberán etiquetar para distinguir entre advertencias, información, errores, etc.
8.5	**Idiomas** La interfaz de usuario del sistema debe ser compatible con español e inglés.
8.6	**Aprendizaje**

8.6.1	La Plataforma deberá ser coherente en cuanto a funcionamiento, apariencia y vocabulario utilizado en todas las áreas de la aplicación.
8.6.2	La Plataforma deberá proporcionar una experiencia intuitiva y un flujo lógico a través de la aplicación. Los pasos que deberá seguir un usuario para completar una tarea o una acción y dónde se encuentra en ese proceso deberán indicarse claramente en la interfaz de usuario de la aplicación.
8.6.3	Las características y la funcionalidad del sistema deberán ser familiares y predecibles.
8.6.4	La Plataforma deberá ser fácil de aprender, eficiente de usar y fácil de recordar.
8.7	**Interfaces de Usuario** Todas las interfaces de usuario del sistema deberán presentarse a través de un navegador web.
8.8	**Resolución del Sitio Web**
8.8.1	Las interfaces de usuario web deberán admitir una resolución mínima de 1024 x 768.
8.8.2	Otras resoluciones de pantalla compatibles.
8.9	**Estándares Web**
8.9.1	La Plataforma deberá usar XHTML 1.1 o HTML 5. El sistema debe usar CSS2.1 o CSS3.
8.9.2	La Plataforma deberá pasar las comprobaciones de validación W3C y CSS.
8.10	**Compatibilidad con dispositivos móviles** Las interfaces externas e internas deberán admitir dispositivos móviles como tabletas.
9.	**Uso**
9.1	**Entidades informantes** La Plataforma deberá poder admitir una población de hasta 30,000 entidades informantes de manera inicial.
9.2	**Monitoreo** La Plataforma deberá proporcionar información de gestión sobre estadísticas del sistema, tendencias de uso y picos de datos.
9.3	**Población de usuarios - Externa** ▪ La Plataforma deberá admitir una población de usuarios de al menos 60,000 usuarios de entidades de informes de manera inicial. ▪ La Plataforma deberá admitir una población de usuarios de al menos 500 usuarios de los CPCEs de manera inicial.
9.4	**Crecimiento de la población de usuarios - Externa** La Plataforma deberá admitir un número cada vez mayor de usuarios externos a medida que otras entidades informantes y usuarios se agreguen con el tiempo.
9.5	**Uso máximo de la población de usuarios - Externo** La Plataforma deberá mantener un buen rendimiento, confiabilidad y resistencia en los puntos de uso máximo, coincidiendo con los plazos para presentar varios reportes.
9.6	**Población de usuarios - Interna** La Plataforma deberá admitir una población de usuarios de aproximadamente 50 usuarios internos de manera inicial.
9.7	**Uso máximo de la población de usuarios - Interno** El sistema debe mantener un buen rendimiento, confiabilidad y resistencia en los puntos de uso máximo, coincidiendo con los plazos para presentar varios reportes.
9.8	**Escalabilidad** La Plataforma deberá ser escalable para un número mínimo de 200,000 entidades informantes.

Requerimientos de los Servicios de Soporte y Mantenimiento

Código	Requerimiento

1.	**Servicio de Soporte**
1.1	Horas normales de servicio son: 8.00 am - 10.00 pm (Argentina) días laborables de Argentina. Horas de servicio extendido: 8.00 am - 5.00 pm (Argentina) sábados, domingos y feriados.
1.2	La disponibilidad operativa de la Plataforma durante las horas de servicio normales y extendido debe ser 99.0%
1.3	El tiempo de recuperación deberá ser como máximo de 6 horas.
1.4	El punto de recuperación de la Plataforma deberá ser 0, es decir, sin pérdida de datos.
1.5	Durante la recuperación de desastres, el tiempo de recuperación no deberá ser más de 24 horas.
1.6	Durante la recuperación de desastres, el punto de recuperación de la Plataforma deberá ser 0, es decir, sin pérdida de datos. Sin embargo, si existe sospecha de corrupción de datos en la Plataforma en caso de un ataque cibernético u otro evento importante, deberá ser posible recuperarla en un punto en el que se sabe que los datos son precisos.
1.7	La consultora deberá brindar apoyo para resolver incidentes y solicitudes planteados por CenFIF: ▪ Se requerirá que el *Help Desk* esté abierto, como mínimo: horas de trabajo de Argentina (de 9:00 a 18:00 de lunes a viernes, días laborables de Argentina). ▪ Sin embargo, el *Help Desk* deberá estar disponible para permitir brindar los servicios con la calidad y disponibilidad especificadas anteriormente durante las horas normales y extendidas de servicio. ▪ Las funciones del *Help Desk* deberán incluir la resolución de incidentes, errores, fallas y consultas, como se define en los siguientes requisitos de servicio. ▪ Esto puede significar que la consultora elija proporcionar un servicio extendido.
1.8	La consultora deberá brindar la funcionalidad del *Help Desk* para que el personal de CenFIF comunique (vía voz, correo electrónico o chat) incidentes y solicitudes, realice su gestión y asegure que CenFIF reciba respuestas dentro de los tiempos de repuesta preestablecidos. El servicio proporcionado deberá tener niveles de servicio en torno a la rapidez con la que se reconoce el incidente o solicitud, se proporcionan soluciones provisorias y/o permanentes: ▪ **Primer nivel de soporte.** Servicio de asistencia funcional y técnica de las consultas más habituales del uso de la Plataforma. ▪ **Segundo nivel de soporte.** Servicio de asistencia funcional y técnica de la Plataforma, siempre y cuando no pueda ser resuelta por el primer nivel de soporte. ▪ **Soporte virtual.** En tiempo real disponible 24 horas, 7 días a la semana, los 365 días del año accesible vía web para el reporte de incidentes y solicitudes que entregará un número de reclamo para su tratamiento. Asimismo, deberá contar con una base de conocimientos (Knowledge Base) en donde existan casos de incidencias resueltos a fin de resolver consultas y/o incidentes de una manera ágil y eficiente, reduciendo así los tiempos de demora en la resolución de los casos de soporte más comunes y frecuentes.
1.9	Los incidentes y solicitudes reportados a la consultora se clasificarán y se priorizarán de acuerdo con el paquete de soporte que mejor se adapte a las horas de servicio y los requisitos de disponibilidad y calidad de CenFIF. Por ejemplo, CenFIF sugiere la priorización de la siguiente manera: ▪ **Prioridad 1 (Crítica):** la Plataforma (o una parte importante de ella) está inactiva, no se puede utilizar o el rendimiento está muy degradado; un proyecto de desarrollo está completamente bloqueado. Tiempo de respuesta: 2 horas. ▪ **Prioridad 2 (Grave):** la Plataforma o los usuarios se ven gravemente afectados; un proyecto de desarrollo se ralentiza drásticamente. Tiempo de respuesta: 4 horas.

	▪ **Prioridad 3 (Intermedio)**: un problema que compromete la productividad del usuario; una funcionalidad no funciona como se encuentra documenta, pero existe una solución alternativa; problema de desarrollo. Tiempo de respuesta: 6 horas. ▪ **Prioridad 4 (Menor):** errores menores que causan un impacto mínimo en los usuarios; consultas sobre la funcionalidad o configuración del producto. Tiempo de respuesta: 8 horas. CenFIF proporcionará detalles razonablemente suficientes del efecto del incidente o solicitud en el funcionamiento de la Plataforma para clasificar el incidente o solicitud como Prioridad 1 - 4 (como se clasificó anteriormente).
1.10	La consultora responderá a todas las comunicaciones de CenFIF de acuerdo con los tiempos de repuesta acordados. ▪ Se considerará que las comunicaciones que reciben una respuesta automática o se colocan en un sistema de espera no han sido respondidas, a menos que se reciban fuera de las horas de soporte, donde se enviará una respuesta automática a CenFIF. ▪ La consultora atenderá todas estas solicitudes al comienzo de las próximas horas de soporte aplicables inmediatas y de acuerdo con los términos de acordados.
1.11	La consultora supervisará sus tiempos de respuesta y proporcionará los resultados de dicho monitoreo a CenFIF de acuerdo con un monitoreo de desempeño.
1.12	CenFIF tendrá derecho (pero no estará obligada) a informar todos los incidentes al *Help Desk*. En cualquier caso, la consultora resolverá todos los incidentes notificados por CenFIF dentro de los tiempos de respuesta acordados.
1.13	La consultora se asegurará de que todas las comunicaciones al *Help Desk* se registren en su registro de *Help Desk*. CenFIF tendrá derechos de verificación con relación al registro de *Help Desk* y la consultora deberá proporcionar toda la evidencia de respaldo.
1.14	Cuando la consultora proporcione una solución provisoria antes de una solución permanente, deberá proporcionar a CenFIF un análisis de impacto y evidencia de las pruebas realizadas por la consultora, a menos que se acuerde lo contrario con CenFIF.
1.15	Cuando la consultora proponga una solución provisoria antes de una solución permanente, CenFIF se reservará el derecho de rechazar dicha solución si no es aceptable para CenFIF (actuando de manera razonable).
1.16	Cuando la consultora proporcione una solución permanente, deberá proporcionar a CenFIF un análisis de impacto y evidencia de las pruebas realizadas por la consultora, a menos que se acuerde lo contrario con CenFIF.
1.17	La consultora proporcionará asistencia técnica *in situ* para la instalación y/o prueba de la solución provisoria o solución permanente suministrada, según sea razonablemente necesario.
1.18	CenFIF (actuando de manera razonable) se reserva el derecho de aplicar las soluciones provisorias o permanentes provistas por la consultora de acuerdo con su propio calendario. ▪ Si CenFIF decide hacerlo, CenFIF considerará que el reloj por el incidente se detuvo en el momento en que la consultora proporcione la solución. ▪ Si CenFIF no ha implementado la solución dentro de las dos (2) semanas posteriores a la recepción de la misma, la consultora podrá comunicarse con CenFIF para averiguar por qué no se ha implementado la solución propuesta y tratar de llegar a una decisión sobre cómo se puede resolver rápidamente el incidente. Si las partes no pueden ponerse de acuerdo sobre la solución que se utilizará para el incidente, el problema se remitirá inmediatamente al procedimiento de escalamiento.
1.19	CenFIF determinará (actuando de manera razonable) cuándo un incidente o solicitud ha sido corregido o resuelto satisfactoriamente.

	Para evitar dudas, si se identificó un nuevo problema no relacionado después de probar una solución brindada, entonces CenFIF deberá informar ese problema como un nuevo incidente en lugar de vincularlo con el incidente original.
1.20	Antes de cualquier entrega de soluciones provisorias o permanentes, correcciones, configuración, desarrollo y/o actualizaciones de software, la consultora deberá realizar pruebas suficientes para garantizar que no se introducirán errores en la Plataforma. La consultora proporcionará evidencia de estas pruebas dentro de las 24 horas si CenFIF lo solicita.
1.21	Antes de implementar las soluciones entregadas en los entornos de producción, CenFIF realizará pruebas suficientes en un entorno de prueba para controlar su calidad. También es responsabilidad de la consultora llevar a cabo las copias de seguridad necesarias del entorno de producción antes de instalar finalmente los nuevos elementos en producción.
1.22	Todas las soluciones, correcciones, configuración o desarrollo y/o actualizaciones de software implementadas por CenFIF estarán cubiertas por los servicios de mantenimiento provistos por la consultora.
1.23	Un error reproducible es un error en uno de los entornos de CenFIF cuya fuente es identificada por el equipo de soporte interno de CenFIF y con respecto al cual CenFIF pueda proporcionar los pasos exactos para reproducir el error.
1.24	Si un error crítico o grave no es reproducible (es decir, que la consultora no puede reproducir el error), la consultora notificará a CenFIF sobre tal evento y, tan pronto como sea razonablemente posible, enviará un experto técnico a CenFIF para investigar el error. CenFIF proporcionará toda la asistencia razonable para ayudar a identificar la causa raíz del error. En el caso de errores no críticos y no reproducibles, las partes razonablemente acordarán el plan de acción adecuado. Los errores no reproducibles no estarán sujetos a los niveles de servicio acordados.
1.25	Si la consultora no puede resolver los incidentes de acuerdo con los tiempos de respuesta acordados, se iniciará un procedimiento de escalamiento para garantizar el involucramiento de personal senior 24 horas después del tiempo de respuesta establecido para incidentes considerados críticos o graves por CenFIF.
1.26	Los cambios a medida en el producto o su configuración por parte de la consultora para cumplir con los requisitos de CenFIF durante los períodos de implementación y garantía deberán ser soportados durante la vigencia del acuerdo y para las versiones posteriores del software, según corresponda.
2.	
2.1	Siempre que lo solicite CenFIF, la consultora deberá proporcionar a CenFIF un informe de estado actualizado con respecto a cada incidente o solicitud dentro de las 8 horas de soporte.
2.2	La consultora deberá proporcionar informes de gestión de una o todas las incidencias o solicitudes registradas en el *Help Desk* a CenFIF dentro de las 8 horas de laborables de realizada la solicitud. Como mínimo, el informe contendrá la siguiente información: ▪ Identificador único. ▪ Fecha y hora de recepción en *Help Desk*. ▪ Si se trata de un incidente o solicitud. ▪ La persona que reporta el incidente o solicitud (con sus datos de contacto). ▪ Detalles del incidente o solicitud. ▪ La prioridad asignada al incidente o solicitud. ▪ La acción que se pretende tomar para resolver el incidente o solicitud. ▪ Reporte (con notas, detalles de contacto, fechas y horas) de cualquier comunicación con CenFIF en relación con el incidente o solicitud. ▪ Si se proporciona una solución provisoria, cuál fue, cuándo se proporcionó y a quién. ▪ Si se proporciona una solución permanente, cuál fue, cuándo se proporcionó y a quién.

	▪ Según corresponda, notas o comentarios sobre cualquier circunstancia mitigante con respecto al incidente. ▪ Según corresponda, los motivos de cualquier incapacidad de la consultora para cumplir con los niveles de servicio para resolver el incidente. Estos informes se proporcionarán en formato PDF y en formato EXCEL, CSV o XML.
3.	**Documentación**
3.1	La consultora proporcionará la documentación de la Plataforma para permitir que el equipo de soporte técnico de CenFIF proporcione soporte de segunda línea. Esta documentación incluirá detalles de toda la funcionalidad del sistema, las opciones de configuración, la ubicación de los archivos de registro y cualquier otra información útil para ellos.
3.2	Cuando un incidente requiera que se actualice la documentación de respaldo, la documentación se deberá actualizar al mismo tiempo que la consultora corrija el incidente (a menos que esto cause demora para liberar la solución).
3.3	La consultora se asegurará de que CenFIF reciba rápidamente los detalles correctos para actualizar la documentación de la Plataforma de modo que se encuentre actualizada en todo momento.
3.4	Cuando exista un error en la documentación, la consultora debe acordar el nivel de criticidad del error con CenFIF y asegurarse de que la documentación se corrija y se entregue a CenFIF de acuerdo con los procesos estándar de la consultora, pero a más tardar 1 día laborable para aquellos errores que estén causando una disrupción en el servicio (por ejemplo, documentación técnica proporcionada a las entidades informantes).
4.	**Versiones de Software**
4.1	CenFIF tendrá control sobre qué versión de software se utilizará durante el acuerdo.
4.2	Por lo tanto, CenFIF no está obligada a aceptar cada nueva versión del software lanzado por la consultora, siempre que CenFIF reconozca que cierta funcionalidad que puede requerir solo puede estar disponible dentro de una versión posterior del software.
4.3	La consultora proporcionará a CenFIF toda la información de actualizaciones y actualizaciones futuras con los documentos de respaldo apropiados, instrucciones completas sobre cómo instalar las actualizaciones y garantizará que todas las configuraciones realizadas hasta la fecha funcionarán con las nuevas actualizaciones o proporcionar un método comprobado para migrar los cambios de configuración a la nueva versión.
4.4	La consultora proporcionará soporte *in situ* para cualquier actualización importante del software.
4.5	La consultora proporcionará al menos 24 meses de notificación por escrito del cese de soporte para la versión del software que CenFIF esté utilizando en su entorno de producción.
4.6	La consultora y el **Ministerio** firmarán un acuerdo de código fuente con modalidad **ESCROW**, cuyo objetivo es garantizar que, en el caso de un cese permanente del soporte a la Plataforma, CenFIF disponga del último código fuente de la Plataforma y las personalizaciones relacionadas. El acuerdo debe garantizar que el código fuente (junto con las actualizaciones periódicas) se deposite con un tercero de confianza, lo que permitirá que el código se libere en caso de que la consultora no pueda continuar dando soporte a la Plataforma.