SELECCIÓN DE CONSULTORES

Solicitud de Propuestas Servicios de Consultoría

Contratación de:

Desarrollo de una nueva versión de SUPRES (Sistema Único de Pago de Recursos Sociales)

Términos de Referencia

SDP: CR-MOF-270101-CS-QCBS

Servicios de consultoría para: Desarrollo de una nueva versión de SUPRES (Sistema Único de Pago de Recursos Sociales)

Contratante: Ministerio de Hacienda de la República de Costa Rica

País: Costa Rica

Emitida el: 25 de abril de 2023

Tabla de Contenidos

TABLA DE ILUSTRACIONES

Acrónimos

API	Application Programming Interfaces (interfaz de programación de aplicaciones).
CCF	Control Contable de Fondos
CCSS	Caja Costarricense de Seguro Social
CEN-CINAI	Centros de Educación y Nutrición-Centros Infantiles de Atención Integral
CGP	Centro de Gestor de Pagos
CONAPAM	Consejo Nacional de la Persona Adulta Mayor
CUT	Cuenta Única del Tesoro
DESAF	Dirección Desarrollo Social y Asignaciones Familiares
DTIC	Dirección de Tecnología de la Información y Comunicación
HD	Hacienda Digital (refiere al Proyecto Hacienda Digital)
HTTP	Hypertext Transfer Protocol, (protocolo de transferencia de hipertextos)
IBAN	International Bank Account Number
IMAS	Instituto Mixto de Ayuda Social
INAMU	Instituto Nacional de las Mujeres
LDAP	Lightweight Directory Access Protocol

MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica
Microsoft ADS	Microsoft Advertising
MH o MdH	Ministerio de Hacienda
MTSS	Ministerio de Trabajo y Seguridad Social
PANI	Patronato Nacional de la Infancia
REST	REpresentational State Transfer
RNC	Régimen no Contributivo de Pensiones
RSS	Really Simple Syndication o Rich Site Summary
SAML	Security Assertion Markup Language
SIGAF	Sistema Integrado de Gestión de Administración Financiera actual del Ministerio de Hacienda
SINIRUBE	Sistema Nacional de Información y Registro Único de Beneficios del Estado
SINPE	Sistema Nacional de Pagos Electrónicos
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture (Arquitectura orientada a los servicios)
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
SUPRES	Sistema Unificado de Pago de Recursos Sociales
TD	Tesoro Digital (actual sistema de pagos utilizado en la Tesorería Nacional)
TN	Tesorería Nacional
UCP	Unidad Coordinadora del Proyecto Hacienda Digital
URL	Uniform Resource Locator
WS	Web Service

Definiciones

Contenedores	Se refiere a paquetes de software que incluyen todos los elementos necesarios para ser ejecutados en cualquier entorno, incluyendo un centro de datos privado, una nube pública o un computador personal.
Centro Gestor de Pagos	Corresponde al Centro Gestor de Pagos en el nuevo sistema integrado de Administración Financiera. Su finalidad es dar servicio financiero y de banco a las entidades que se les ha depositado en cuentas registrales de la Caja Única, así como el registro, verificación, consolidación y ejecución de todos los pagos de subsidios sociales monetarios que emitan las entidades gestoras de dichos servicios.
Hacienda Digital	Proyecto de Hacienda Digital para el Bicentenario.
Serverless	Un tipo de microservicio que permite al proveedor de nube cobrar solo la utilización real del servidor, optimizando el costo de CPU.

1. Introducción

En el presente documento se plasman los requerimientos técnicos necesarios para el desarrollo de una nueva versión de **SUPRES** (**Sistema Único de Pago de Recursos Sociales**), y sus respectivas consideraciones para su implementación, interoperando con el Tesoro Digital y las condiciones para que opere interoperando con el Centro Gestor de Pagos (CGP) en el contexto de implementación del proyecto de Hacienda Digital actualmente en curso.

2. ANTECEDENTES Y JUSTIFICACIÓN

El SUPRES , como su nombre lo indica busca centralizar la gestión de los pagos de beneficios sociales. aquí es importante hacer énfasis en la gestión del pago de beneficios en pro de mejorar la calidad del pago, el Nuevo SUPRES se concibe como una aplicación desacoplada, que debe ser diseñada para poder interoperar con la actual versión del Tesoro Digital y en el futuro con el Centro Gestor de Pagos de Hacienda Digital que operan de forma integrada con el SINPE. El Sistema Nacional de Pagos Electrónicos (SINPE) es una plataforma tecnológica desarrollada y administrada por el Banco Central de Costa Rica, que conecta a entidades financieras e instituciones públicas del país a través de una red privada de telecomunicaciones, la cual les permite realizar la movilización electrónica de fondos entre cuentas clientes y participar en los mercados de negociación que organiza el Banco Central de Costa Rica mediante esa plataforma.

Si bien es cierto el actual SUPRES ha resuelto los principales problemas identificados como:

> **La inexistencia de un mecanismo centralizado y automático de validación de las órdenes de pago a beneficiarios genera ineficiencias en el proceso.** Los archivos de pago que las entidades elaboran y envían a la banca comercial para soportar los pagos a beneficiarios de programas de protección social no pasan por un control previo de validación de los beneficiarios. Así, a pesar de la existencia de un sistema como el SINIRUBE (que tiene como propósito mantener una base de datos actualizada con la información de la población objetivo que requieren subsidios o atención del Estado por encontrarse en condición de pobreza), y de las reglas sobre registro de información en este sistema, no se cruza ni se verifica entre la entidad proponente de beneficios sociales y el SINIRUBE, la validez de la información sobre beneficiarios, beneficios y montos que cada entidad registra en los archivos de pago. Con ello, se producen los siguientes riesgos operativos: duplicación de beneficios por beneficiario; entrega de beneficios a quien no corresponda o en montos indebidos; entrega de un total de beneficios a grupos familiares en montos

superiores a los esperados; o generación de pagos a beneficiarios inexistentes o que no cumplen con las condiciones establecidas por el programa social.

Si bien es cierto que el uso de la banca comercial facilita la transparencia y trazabilidad del proceso de pagos, en la actualidad no existe para los pagos de beneficios sociales algo similar a lo expuesto anteriormente, ante lo cual nació una necesidad de mejora respecto a este tipo de pagos. Debido al esquema descentralizado existente de pagos asociados a programas de protección social, la TN pierde la trazabilidad de los recursos destinados al pago de los beneficiarios transferidos desde las cuentas de Caja Única de las entidades hacia la banca comercial. Dado este esquema, no hay información centralizada sobre beneficios efectivamente abonados y aquellos pendientes, como tampoco hay una devolución a la TN de los fondos de los beneficios que no fueron pagados. Con ello, se dificulta el control y la toma de decisiones de las entidades centrales que transfieren recursos para este tipo de programas, como también se limita la rendición de cuentas sobre el uso de tales recursos.

Pérdida de oportunidad para promover la igualdad de género mediante la inclusión financiera de las mujeres titulares de los beneficios de los programas de transferencias de ingresos. Esto se refleja en las siguientes cifras. La brecha en la titularidad de una cuenta entre hombres y mujeres fue en Costa Rica en el año 2017 de 14 p.p. entre hombres (75%) y mujeres (61%). También en el año 2017, el 27% de los hombres y el 22% de las mujeres mayores de 15 años manifestaron ahorrar en una institución financiera, mientras tomaron préstamos en una institución financiera el 25% de ellos y solo el 18% de ellas. Por medio de esta herramienta informática a futuro y con la información recopilada, se podrían obtener reportes específicos, como, por ejemplo: reporte de género, para motivar políticas o acciones concretas para promover este tipo de pago en igualdad de género de beneficio social.

Los beneficios del nuevo SUPRES pueden resumirse en los siguientes:

- Validación de la información previo al pago de los beneficios de recursos sociales
- Centralización de información de pagos de beneficios de recursos sociales

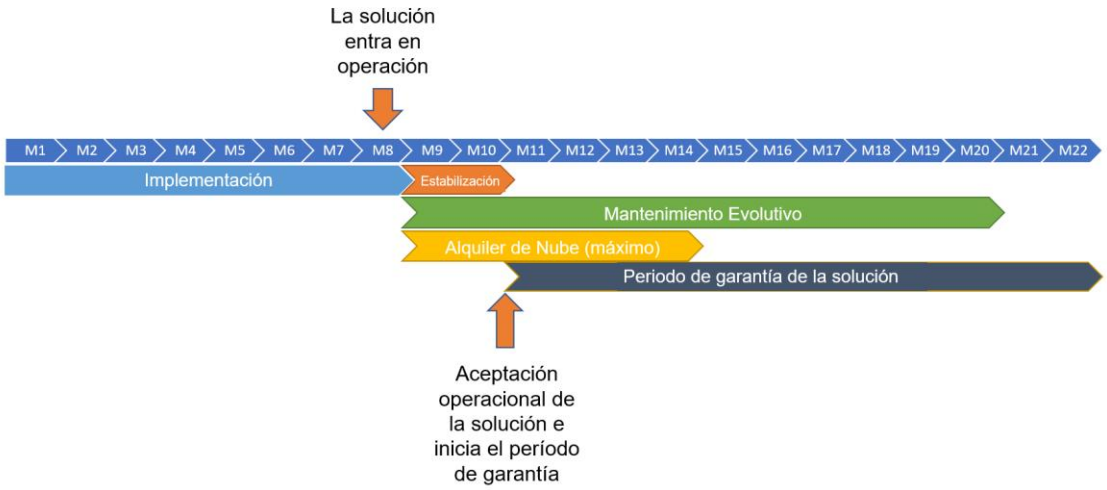
SUPRES actualmente se encuentra implementado y acoplado al Tesoro Digital, lo cual a futuro será reemplazado por el Centro Gestor de Pagos del proyecto de Hacienda Digital y considerando que el diseño conceptual de CGP no considera las peculiaridades del pago de beneficios, obliga a desarrollar una nueva versión de SUPRES que opere como un sistema independiente que además amplié la cobertura de pagos directos (se realizan a una persona en particular) a pagos no directos (son pagos a las diferentes instituciones para que estas los distribuyan a la población de su cobertura), que actualmente no puede cubrir por restricciones en su diseño.

3. OBJETO DE LA CONTRATACIÓN

Contratar el desarrollo, implementación y puesta en producción y adaptación evolutiva de la solución "**Sistema Único de Pago de Recursos Sociales (SUPRES)**" que centralice la gestión de los pagos de beneficios sociales, interoperando con Tesoro Digital y a su vez con el SINIRUBE y que mantenga las condiciones para operar con el Centro Gestión de Pagos, en el contexto de implementación del proyecto de Hacienda Digital actualmente en curso.

4. PLAZO DE LA CONTRATACIÓN

El plazo de la contratación se estima en **22 meses** distribuidos de la siguiente manera, (ver figura adjunta):



La Fase de Implementación tiene una duración de **08 meses** y comprende las etapas de entendimiento, planificación, desarrollo, pruebas e implementación de acuerdo con los requerimientos detallados en este documento. Incluye además la capacitación, transferencia de conocimiento al equipo técnico del Ministerio de Hacienda. Esta etapa contempla los requerimientos del SUPRES operando con el actual Tesoro Digital (TD). En el apartado *5.2.1. Explicación de los procesos*, se describen las macro actividades que tiene que hacer el Nuevo SUPRES operando con Tesoro Digital.

Seguidamente viene la Fase de Estabilización, la cual será de **02 meses**, durante los cuales la firma consultora debe realizar las tareas necesarias para estabilizar el funcionamiento de la solución implementada. Al cabo de la culminación exitosa de esta etapa, se brinda la Aceptación Operacional.

Existirá además una Fase de Mantenimiento Evolutivo, la cual se inicia a partir de la finalización de la Fase de Implementación y se prolonga durante **12 meses** prorrogables por la vida del sistema. Durante esta fase el Ministerio de Hacienda podría solicitar ajustes a la solución con cargo a la bolsa de horas del proyecto. En el apartado *5.2.1. Explicación de los procesos*, se describen las macro actividades que tiene que hacer el Nuevo SUPRES operando con el nuevo sistema de Hacienda Digital.

Habrá también una Fase de Alquiler de Nube que constará de un plazo máximo de **6 meses**, la cual inicia a partir de la finalización de la Fase de Implementación, durante la cual la firma consultora (en la eventualidad de que el Ministerio de Hacienda no haya aprovisionado el servicio de nube al finalizar la Fase de Implementación) deberá iniciar la misma en una instancia de nube provista por él, debiendo realizar la migración a la nube definida por el Ministerio de Hacienda en el momento que se le indique. Si al iniciar con la parametrización de la solución el Ministerio de Hacienda ha aprovisionado el servicio de nube, lo indicado no será requerido y el MH no pagará por este rubro. En caso se utilice el servicio por un plazo menor a 6 meses se pagará por el tiempo utilizado. Al cabo de dicho plazo, los sistemas desarrollados, con todos sus ambientes deberán ser trasladados a la nube que indique el Ministerio de Hacienda.

La firma consultora deberá brindar una garantía de **12 meses** sobre el software desarrollado, a partir de la finalización de la Fase de Estabilización, período durante el cual deberá realizar correcciones sobre errores que se presenten en la solución desarrollada. Las mejoras realizadas a través del Mantenimiento Evolutivo estarán igualmente garantizadas hasta la finalización de los 12 meses indicados en este párrafo.

5. MODELO CONCEPTUAL DE SUPRES

5.1 Flujo Actual de Proceso de Pagos Sociales sin SUPRES

El sistema Tesoro Digital ofrece a las entidades una página transaccional para administrar sus cuentas de Caja Única, permitiéndoles efectuar operaciones como las siguientes: pagos electrónicos y cobros mediante débitos directos a cuentas en cualquier entidad financiera del país en tiempo real; transacciones en línea entre cuentas de Caja Única, consulta de saldos y movimientos en línea; y firma digital.

A continuación, se presenta una descripción del flujo habitual correspondiente al proceso de pagos asociado a un programa de protección social basado en transferencias monetarias para el caso de tres entidades: IMAS (Protege y promueve, de manera inclusiva y solidaria, el desarrollo de la población en situación de pobreza y pobreza extrema, mediante programas y proyectos, desde un abordaje multidimensional), PANI (Institución encargada de velar por los derechos de la niñez y la adolescencia) e INAMU (Institución que promueve y tutela los derechos humanos de las mujeres, pone a disposición de la sociedad costarricense y de las mujeres en particular, información acerca de sus áreas de trabajo y los servicios ofrecidos). A lo largo de la sección, se

señalan algunas variaciones en el flujo identificadas en los casos del IMAS, PANI, e INAMU. En la Figura 1, se esquematiza el flujo habitual.

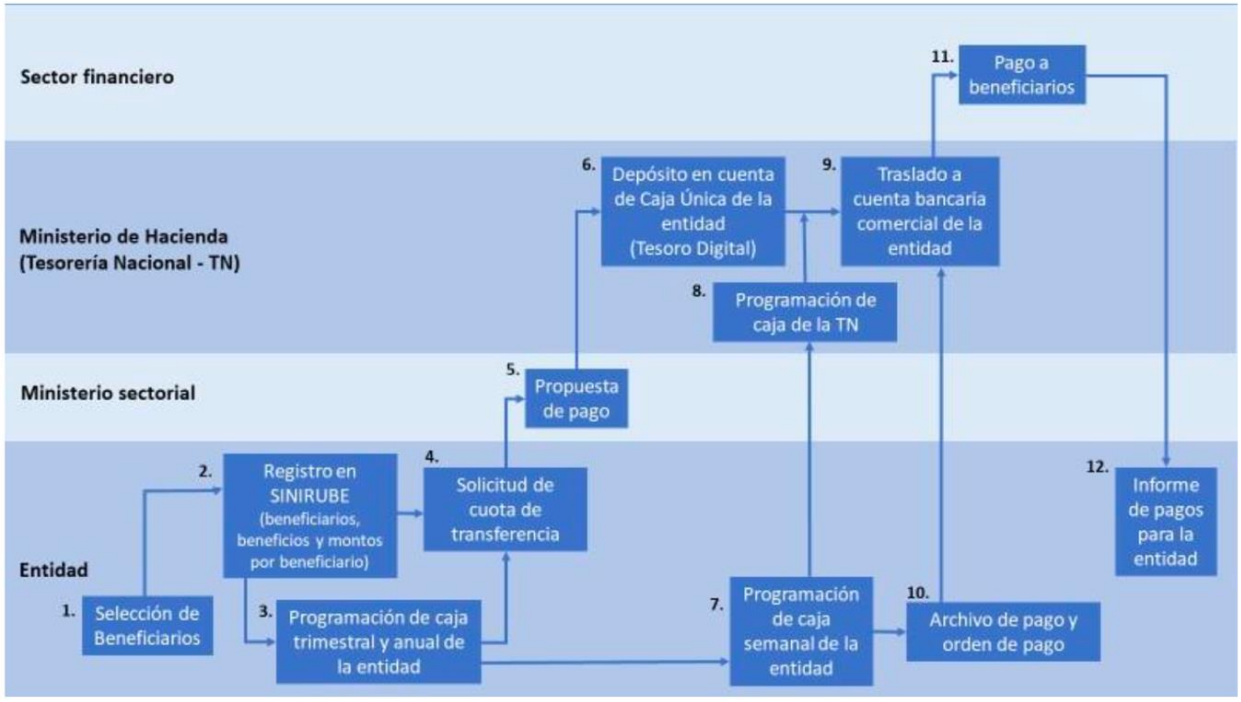


Ilustración 1 - Flujo actual del proceso de pagos sociales (en este flujo no hay partición de SUPRES)

Flujo del proceso de pagos asociado a un programa de protección social basado en transferencias monetarias

1. El proceso se inicia con la definición y validación de los beneficios y beneficiarios de cada programa de protección social, fijando el monto de recursos a ser transferido (pagado) a cada beneficiario. Esta tarea es responsabilidad de la entidad que gestiona cada programa, siguiendo la normativa vigente.

2. La información sobre beneficiarios, tipo de beneficios y monto asociado a los beneficios debe ser registrada por cada entidad en el Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (SINIRUBE). [1]El registro centralizado de información que exige el SINIRUBE permitiría identificar la totalidad de beneficios (tipo y monto) que recibe cada uno de los beneficiarios de programas de protección social (o el grupo familiar a los que estos pertenezcan), incluyendo aquellos basados en transferencias monetarias. Sin embargo, actualmente, el PANI no cumple el requisito de registro en el SINIRUBE de sus beneficiarios.

[1] Para más detalles ver www.sinirube.go.cr

3. Mensualmente, y de acuerdo con el monto de pagos generado por los beneficios asignados de los programas protección social a su cargo, la entidad actualiza su programación de pagos a beneficiarios y la incorpora en una actualización de su programación de caja trimestral y anual (una proyección indicativa del flujo de caja de la entidad en dichos horizontes de tiempo), que es enviada a la TN vía correo electrónico en archivo PDF.

   En el horizonte anual, la programación de caja se expone por mes. En el horizonte trimestral, se expone por semana o por día, dependiendo si la entidad es catalogada por la TN como de bajo o alto volumen, respectivamente. Para ambos tipos de entidades en la programación de caja se ofrece información agregada sobre ingresos y egresos. En el caso de los ingresos, traslados desde el sistema financiero nacional, transferencias del gobierno central y traslados desde cuentas de Caja Única de otras entidades. En el caso de los egresos, traslados hacia el sistema financiero nacional, devoluciones al Fondo General y traslados hacia cuentas de Caja Única de otras entidades.

4. Considerando su programación de caja, las entidades participantes de beneficio social tales como: PANI, IMAS entre otras, hacen una solicitud de cuota de transferencia al ministerio sectorial respectivo[2]. En la solicitud, la entidad informa sobre el monto total requerido para pagos en el mes correspondiente. Esta solicitud se hace por oficio, correo electrónico u otros medios propios del sector.

5. El ministerio sectorial (ente concedente) revisa la solicitud de cuota de transferencia de la entidad y, una vez validada, envía una propuesta de pago a la TN a través del Sistema Integrado de Gestión de Administración Financiera (SIGAF). En la propuesta, se informa sobre el monto para pagos a ser transferido a la entidad el siguiente mes y la cuenta de Caja Única de dicha entidad donde debe ser depositado el monto mencionado (en pocos casos, el depósito se hace a cuentas bancarias comerciales de las entidades). Por decisión del ministerio sectorial, este monto puede ser inferior al solicitado por la entidad, por ejemplo, por motivos de disponibilidad de flujo de caja.

6. Después de validar la propuesta de pago, la TN deposita la totalidad del monto propuesto por el ministerio sectorial en la cuenta de Caja Única de la entidad solicitante, en Tesoro Digital.

7. Con base en su programación de caja trimestral y anual, la entidad prepara y envía a la TN su programación de caja diaria para la siguiente semana, incluyendo lo relativo a pagos a beneficiarios de los programas de protección social. Esta programación se entrega en un archivo de Excel vía correo electrónico.

[2] Las entidades responsables de los programas sociales dependen de un Ministerio sectorial a nivel presupuestario.

8. La TN, utilizando la plataforma Tesoro Digital, y considerando la programación de caja de la entidad en sus diferentes horizontes (semanal, trimestral y anual), transfiere a una cuenta bancaria comercial de la entidad los recursos que fueron depositados en la cuenta de Caja Única de la misma entidad según la propuesta del ministerio sectorial. Este traslado se hace a través del Sistema Nacional de Pagos Electrónicos (SINPE), y puede ser total o diferirse a lo largo del mes respectivo según la programación de caja de la TN.

9. Con los recursos disponibles en su cuenta bancaria comercial, la entidad ordena al banco efectuar los pagos a beneficiarios de acuerdo con el convenio que haya firmado con dicho banco. Para proceder al pago, la entidad envía al banco un archivo para pagos con la siguiente información: nombre del beneficiario (o de aquel a quien se otorgue el derecho para recibir el pago del beneficiario), número de la cuenta bancaria comercial del beneficiario (en caso de que tenga cuenta) y monto a pagar por beneficiario.

    Cabe señalar que la plataforma Tesoro Digital de la TN tiene la posibilidad de hacer pagos electrónicos a los beneficiarios de manera directa desde la cuenta de Caja Única de la entidad, evitando el paso por cuentas bancarias comerciales de las entidades (y el costo en tiempo y dinero que ello implica). Sin embargo, este procedimiento no se ha generalizado aún dado que el modelo de gestión para el pago de recurso social es de reciente creación.

10. Recibida la orden de pago, el banco efectúa los pagos a los beneficiarios mediante el canal definido para ello. Los medios de pago existentes en la actualidad son

    i) internet *banking*, donde se abre una cuenta de ahorros con tarjeta débito para el beneficiario, cuenta donde se depositan los pagos;
    ii) tarjetas prepago, que sirven como medio para que el beneficiario retire el dinero correspondiente a sus pagos de la cuenta bancaria comercial de la entidad;
    iii) cheques;
    iv) pagos por ventanilla en sucursales bancarias; y
    v) efectivo.

11. Realizados los pagos a los beneficiarios, el banco envía a la entidad información sobre los beneficiarios que recibieron el pago, los montos pagados por beneficiario y los beneficiarios que no recibieron el pago.

12. Cuando los beneficiarios no reciben los pagos correspondientes, los montos respectivos permanecen en la cuenta bancaria comercial de la entidad, y no regresan a su cuenta de Caja Única en la TN.

Existe una variación en el caso del IMAS cuando el canal de pagos corresponde a tarjetas prepago. En este caso, el IMAS transfiere los recursos desde su cuenta bancaria comercial a las cuentas bancarias comerciales de sus oficinas regionales. Luego, estas oficinas preparan los archivos para pagos a beneficiarios y los envían directamente al banco en el momento de

dar a este la orden de pago. Finalmente, el banco informa a las oficinas regionales respectivas sobre beneficiarios que recibieron el pago, montos pagados por beneficiario y beneficiarios que no recibieron el pago. Los montos no pagados permanecen en las cuentas bancarias comerciales de las oficinas regionales.

En el INAMU, también se observa una variación con respecto al procedimiento expuesto. En este caso, el pago a las beneficiarias del programa FOMUJERES (único programa basado en transferencias monetarias gestionado por el INAMU) se hace directamente desde la cuenta en Caja Única del INAMU vía SINPE, de manera que los recursos no pasan por una cuenta bancaria comercial de la entidad llegando directamente a las beneficiarias mediante transferencia electrónica directamente desde la cuenta de Caja Única del INAMU vía SINPE.

5.2 Modelo de Interacción entre actores relevantes

El nuevo SUPRES estará inmenso en un ecosistema en donde se requiere la operación conjunta de instituciones y sus sistemas. Esto se inicia desde que la institución genera sus respectivos procesos que sirven de base para la emisión de las solicitudes de pago, esta información, que para efectos del SUPRES se denomina información complementaria para el pago. El sistema validará previamente aquellas reglas de control acordadas con las instituciones originadoras del pago y el sistema SINIRUBE. Lo anterior permite la trazabilidad y transparencia en el otorgamiento, pago y remisión posterior de información a los gestores o proponentes de los pagos, así como a los beneficiarios de estos. Asimismo, el sistema permitirá una mayor eficiencia en la gestión de estos pagos, al realizarlos desde la CUT evitando el traslado hacia cuentas bancarias pagadoras y propiciará la utilización de medios de pago electrónicos.

En este contexto la nueva versión del SUPRES se define como un sistema desacoplado de los sistemas de los que se nutre de información, aplica reglas de decisión sobre si corresponde continuar o no con un pago, y nutre información a los sistemas externos e informa a los beneficiarios de los pagos.

Adicionalmente, existen dos grandes diferencias respecto del origen de los pagos que afectan directamente la funcionalidad de SUPRES, esto es principalmente porque no necesariamente los pagos de beneficios sociales se pagan con carga al presupuesto de la república, sin embargo, sus recursos sí están en la CUT, para efectos de esta especificación se usará el concepto de Integración, donde:

Sin Integración: Significa que los beneficios a pagar son con cargo al presupuesto nacional, por lo tanto, para ser pagados deben cumplir con todos los momentos del gasto que la administración financiera exige y la instrucción de pago debe salir de SIGAF cuando SUPRES opere con TD y cuando se trata de HD desde el Sistema de Administración Financiera que se adquiera.

Con Integración: Significa que los beneficios a pagar son con cargo a recursos de terceros depositados a cuentas de Caja Única mediante la aprobación de un presupuesto público. En este

caso la instrucción de pago cae directamente en el TD o Gestor de Pagos, sin ningún tipo de interacción con el sistema de Administración Financiera (SIGAF o el que se adquiera con HD)

Se muestran los 2 posibles flujos, donde la diferencia entre ambos se observa en los sistemas con que interactúa, no así en las funcionalidades de SUPRES que son las mismas independientemente del origen de los fondos administrados. Los flujos se describen a continuación:

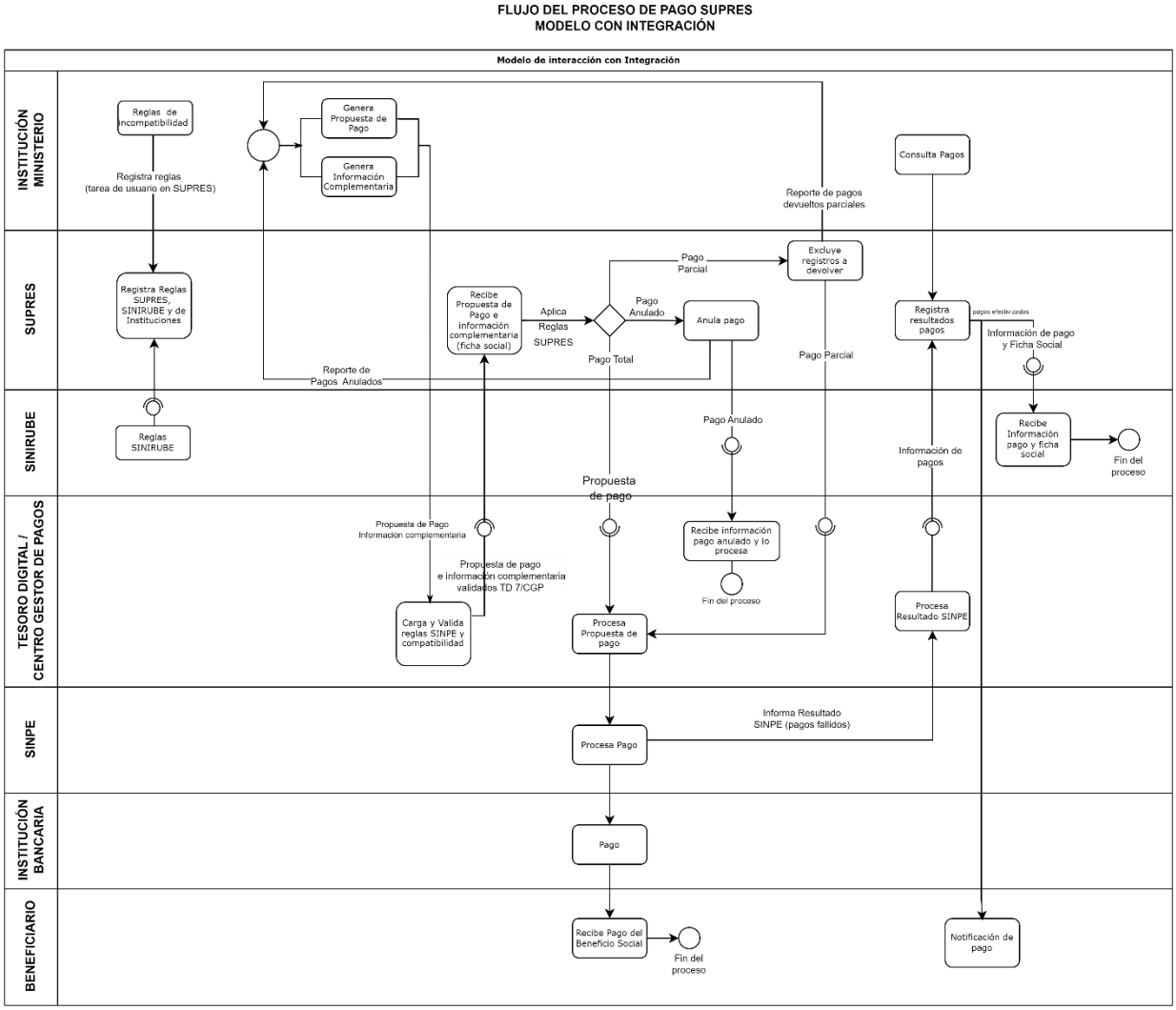


Ilustración 2 - Flujo SUPRES con Integración (ver apartado 5.2)

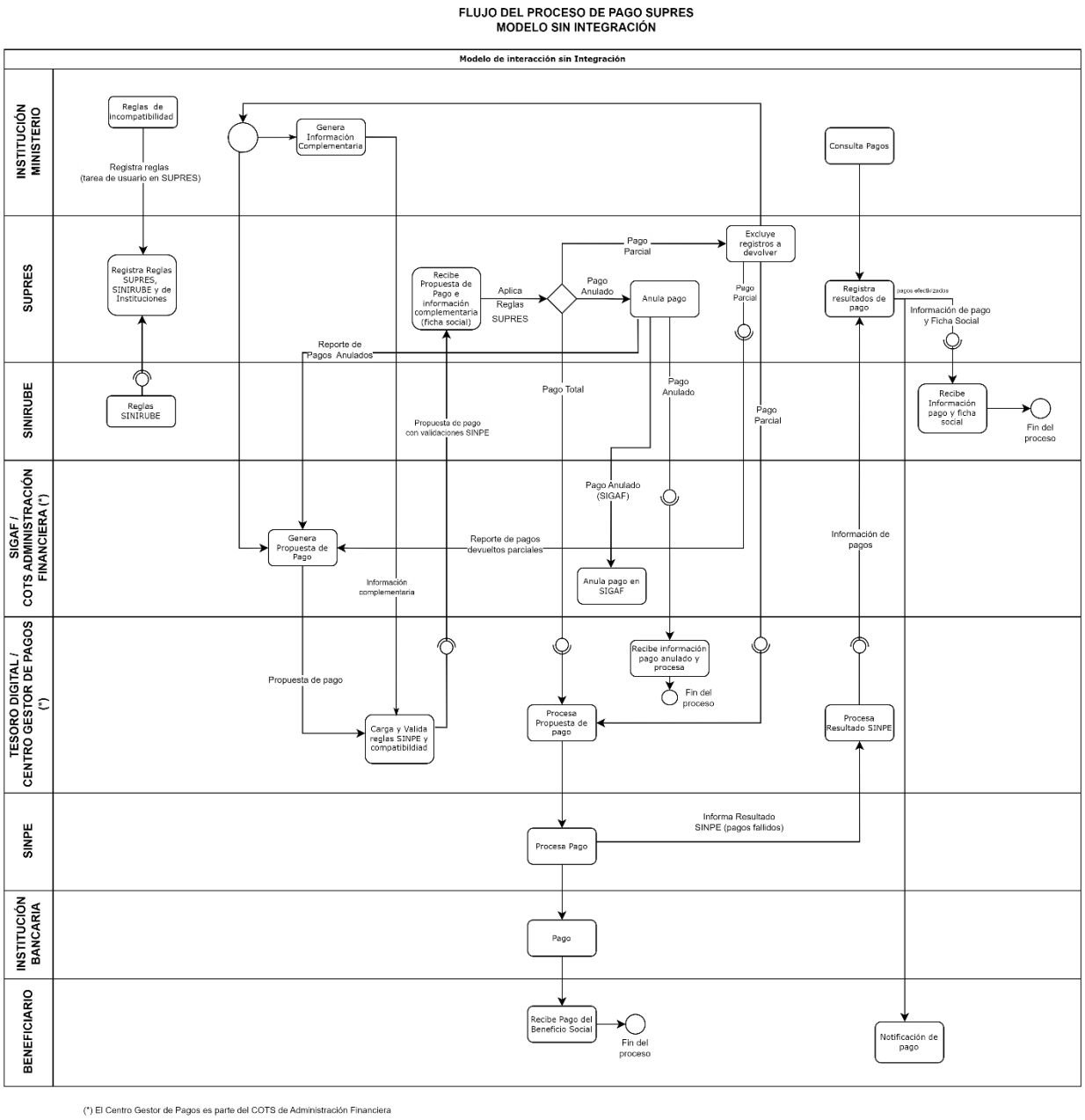


Ilustración 3 - Flujo SUPRES sin integración (ver apartado 5.2)

Complementando, el diseño concibe en su definición las restricciones como:

a) Se debe impactar lo menos posible los procesos de emisión de solicitudes de pago actual y en concreto no se pueden tocar funcionalidades de SIGAF, por lo tanto, este proceso se debe mantener como hasta ahora se viene operando y solo se pueden realizar cambios menores al TD.

b) Mantener el principio de eficiencia y eficacia, lo que se traduce en que cada sistema/actor realice las actividades que le competen (TD procese solicitudes de pago, SINPE abone en cuenta y por su parte SUPRES sea el nexo entre lo social y financiero).

5.2.1 Explicación de los procesos

La presente sección explica las macro actividades que tiene que hacer el Nuevo SUPRES y sus Posibles Diferencias dependiendo del flujo en que esté operando (con el actual Tesoro Digital o con el nuevo sistema de Hacienda Digital):

Macro Proceso	Con Integración	Sin Integración
Propuesta de pago	**Con Sistemas Actuales del MH** La institución registra/carga su propuesta de pago en el "canal SUPRES" del Web Banking del Tesoro Digital **Con COTS Hacienda Digital** La institución registra/carga su propuesta de pago en el Portal de Servicios Financieros del Centro Gestor de Pagos. (El Centro Gestor de pagos es parte del COTS financiero de HD)	**Con Sistemas Actuales del MH** La institución genera su propuesta de pago en el SIGAF, donde mediante un sitio seguro se envía a Tesoro Digital. **Con COTS Hacienda Digital** La institución genera su propuesta de pago en el COTS financiero, desde donde por integración se envía al Centro Gestor de Pagos.
Información complementaria	**Con Sistemas Actuales del MH** La institución registra/carga su información complementaria en el "canal SUPRES" del Web Banking del Tesoro Digital **Con COTS Hacienda Digital** La institución registra/carga su información complementaria en el Portal de Servicios Financieros del Centro Gestor de Pagos del COTS	Ídem a con integración
Carga y Validación reglas SINPE y compatibilidad	**Con Sistemas Actuales del MH** Tesoro Digital valida de forma automática las reglas SINPE (p.e. formato de archivo) y compatibilidad del archivo complementario con el de propuesta de pago (p.e. valida nombre, id)	Ídem a con integración

	Con COTS Hacienda Digital El Centro Gestor de Pagos realizará las mismas validaciones actuales (reglas SINPE y compatibilidad archivo).	
Recepción de propuesta de pago e información complementaria	**Con Sistemas Actuales del MH** La información se recibe en SUPRES por interoperabilidad con Tesoro Digital **Con COTS Hacienda Digital** La información se recibe en SUPRES por interoperabilidad con el Centro Gestor de Pagos del COTS financiero.	Ídem a con integración
Aplica Reglas SUPRES	SUPRES debe tener la capacidad de aplicar reglas previamente configuradas[3]: - Reglas SINIRUBE - Reglas de Instituciones - Reglas SUPRES De la aplicación de estas reglas el resultado puede ser: - Pago Total - Pago Parcial - Pago Anulado	Ídem a con integración
Pago Total	**Con Sistemas Actuales del MH** SUPRES envía por Interoperabilidad a Tesoro Digital el Ok para el procesamiento del pago. **Con COTS Hacienda Digital** SUPRES envía por Interoperabilidad al Centro Gestor de Pagos el Ok para el procesamiento del pago.	Ídem a con integración
Pago Parcial	SUPRES excluye los registros que generaron error.	Ídem a con integración

[3] Ver más abajo la explicación de este proceso

Exclusión de registros a devolver	Los registros excluidos serán informados a las instituciones mediante un reporte del SUPRES, a efectos que éstos puedan corregir e incorporar a una nueva propuesta de pago (información de pago e información complementaria) **Con Sistemas Actuales del MH** SUPRES informa por interoperabilidad a TD para que éste procese los pagos correctos del archivo. **Con COTS Hacienda Digital** SUPRES informa por interoperabilidad al Centro Gestor de Pagos para que éste procese los pagos correctos del archivo.	**Con Sistemas Actuales del MH** SUPRES debe informar a SIGAF (proceso de registro manual) **Con COTS Hacienda Digital** SUPRES debe informar al módulo del COTS financiero correspondiente (interoperabilidad).
Pago Anulado	SUPRES anula el pago y emite un reporte de Pago Anulado para informar a instituciones. **Con Sistemas Actuales del MH** SUPRES informa por interoperabilidad a TD la anulación del pago **Con COTS Hacienda Digital** SUPRES informa por interoperabilidad al Centro Gestor de Pagos.	Ídem a con integración **Con Sistemas Actuales del MH** SUPRES debe informar a SIGAF (proceso de registro manual) **Con COTS Hacienda Digital** SUPRES informa por interoperabilidad al Centro Gestor de Pagos, quien por integración informa al módulo del COTS financiero correspondiente.
Información de Pagos SINPE	**Con Sistemas Actuales del MH** TD procesa el resultado SINPE e informa por interoperabilidad al SUPRES. SUPRES genera un reporte para consulta por parte de las instituciones y las notifica. **Con COTS Hacienda Digital**	Ídem a con integración

	Centro Gestor de Pagos procesa el resultado SINPE e informa por interoperabilidad al SUPRES. SUPRES genera un reporte para consulta por parte de las instituciones y las notifica.	
Procesamiento de Pago SINPE	SINPE realiza el procesamiento habitual de pagos	Ídem a con integración
Pago	Proceso habitual de la institución bancaria que recibe de SINPE el pago a realizar al beneficiario	Ídem a con integración
Abono en cuentas	Proceso habitual Institución bancaria	Ídem a con integración
Recepción del Pago de Beneficio social	Proceso habitual de la institución bancaria informando el abono en cuenta del beneficiario	Ídem a con integración
Notificación Beneficio	SUPRES con la información enriquecida (complementaria) notifica al beneficiario sobre el programa beneficio que se pagó	Ídem a con integración
Envío de resultado de pago y ficha social a SINIRUBE	SUPRES informa por interoperabilidad a SINIRUBE el resultado del pago, y la ficha social (información complementaria).	Ídem a con integración

5.2.2 Interfases a desarrollar

El sistema SUPRES deberá contar con el siguiente conjunto de interfaces requeridas. El proveedor deberá realizar la implementación cumpliendo lo que especifica el apartado 7.21 Interoperabilidad del documento de términos de referencia, de manera tal que la implementación resulte desacoplada del sistema de información origen o destino de la interfaz. De esta forma la implementación en primera instancia se realizará con los sistemas actuales (Tesoro Digital) y posteriormente las mismas interfaces deberán funcionar con la implementación del nuevo sistema COTS de Administración Financiera desarrollado en el Proyecto Hacienda Digital.

	Integración	**Sistema origen**	**Sistema destino**	**Contenido**	**Métodos**
1	Reglas SINIRUBE	SINIRUBE	SUPRES	Reglas de SINIRUBE	• Envío de nuevas reglas de validación SINIRUBE

	Integración	Sistema origen	Sistema destino	Contenido	Métodos
2	Propuesta de pago e información complementaria	TD / Gestor de Pagos	SUPRES	Información de la propuesta de pago que se realiza e información complementaria	• Envío de propuesta de pago • Envío de información complementaria
3	Pago Total	SUPRES	TD / Gestor de Pagos	Ok a la información de pago (total)	• Envía el Ok
4	Pago Anulado	Nuevo SUPRES	TD / Gestor de Pagos	Aviso de que la propuesta de pago debe ser anulada	• Aviso de anulación
5	Pago Parcial	SUPRES	TD / Gestor de Pagos	Información del Pago parcial	• Envía la información del pago parcial (propuesta de pago original excluidos los registros con error)
6	Pago Parcial – registros excluidos	SUPRES	COTS financiero	Información excluida del registro de pago	• Envía la información excluida.
7	Información de pagos fallidos	TD o Gestor de Pagos	SUPRES	Información de los pagos fallidos en SINPE	• Información de los pagos fallido
8	Información de pagos y ficha social	SUPRES	SINIRUBE	Información de pagos realizados e información complementaria (ficha social)	• Información de los pagos realizados • Información complementaria

6. REQUERIMIENTOS FUNCIONALES

RF-SUPRES.01	El sistema debe permitir el registro de la información de pago e información complementaria de subsidios sociales monetarios que emitan las entidades

	que gestionan recursos en la Cuenta Única del Tesoro (CUT) provenientes del presupuesto nacional o de fondos de terceros.
RF-SUPRES.02	El sistema debe registrar y almacenar las reglas de control que aplicará a cada información de pago: - Reglas acordadas con las instituciones (registradas por un usuario de la institución en SUPRES) - Reglas SINIRUBE (registradas por interoperabilidad) - Reglas SUPRES (registradas por un usuario de la TN en SUPRES)
RF-SUPRES.03	El sistema debe proveer un motor de reglas parametrizable y programables que permita incorporar reglas sin necesidad de actualizar el sistema
RF-SUPRES.04	El sistema debe validar las reglas de control una vez cargada la información del pago e información complementaria. Debe tener la capacidad de manejar en forma parametrizable la severidad de la respuesta como: Severa Alta: No permite el tránsito de esa transacción Severidad Media: Advierte situación, pero no evita el tránsito de la transacción Severidad Baja: Información adicional que no afecta el proceso.
RF-SUPRES.05	El sistema debe permitir excluir de la propuesta de pago todos aquellos registros que cumplen con severidad alta, generando un ajuste por los registros que no se pagarán. Este ajuste debe quedar registrado en el sistema. Em esta situación, puede darse: - Pago Parcial (con exclusión de los registros a devolver, el resto de registros sigue su proceso para el pago) - Pago Anulado (no continúa el proceso)
RF-SUPRES.06	El sistema debe proveer mecanismos manuales de reversión de pago en al caso que no se pueda invocar la reversión en forma automática.
RF-SUPRES.07	El sistema debe emitir un reporte de los registros excluidos o pago anulado para ser consultado por la institución.
RF-SUPRES.08	El sistema debe tener la capacidad de procesar pagos Directos y No Directos, identificando qué beneficiarios agrupa un pago, de forma de poder informar a SINIRUBE a quien se le realizo la trasferencia y su correspondencia en monto de los beneficiarios que la componen. Se entiende por pago directo aquella transferencia que es dirigida a quien tiene asignado el beneficio; se entiende como pago No Directo cuando quien recibe la transferencia no es el beneficiario del subsidio, además el monto a transferir puede ser para uno o más beneficiarios.
RF-SUPRES.09	El sistema debe notificar a las instituciones cuando un pago no pudo ser procesado por SINPE (pagos fallidos). Esta información será visualizada por las instituciones mediante un reporte en el sistema.
RF-SUPRES.10	El sistema debe generar para enviar a SINIRUBE los resultados de los pagos e información enriquecida (información complementaria).
RF-SUPRES.11	El sistema debe prever y gestionar mecanismos de notificación a los beneficiarios que recibieron su pago, esta notificación debe incluir el debido

	detalle del pago utilizar diferentes canales que se parametricen para cada programa. Deberá considerar para estos efectos diferentes medios de notificación, entre ellos el mensaje de texto a teléfonos móviles, correo electrónico, mensaje WS y otros que se lleguen a identificar.
RF-SUPRES.12	El sistema debe generar un reporte a las instituciones gestoras de los pagos que contenga la información necesaria para sus procesos de registros y afectaciones presupuestarias y contables que éstas deban realizar y deberán estar referenciadas a la información recibida de la propuesta de pagos.
RF-SUPRES.13	**Consultas y Reportes.** El sistema debe considerar tanto reportes operativos como reportes analíticos. En cuanto a los primeros, se prevé un máximo de 10 reportes. Respecto a los reportes analíticos, el sistema deberá proveer mecanismos de integración con un módulo de inteligencia de negocio que permita por medio de cubos de información, filtrar datos y emitir reportes (impresos y exportables en diferentes formatos), que al menos contengan, por ejemplo, las siguientes opciones: a. Pagos en un periodo definido por código de entidad. b. Pagos en un periodo definido por código de programa. c. Pagos en un periodo definido por beneficiario. d. Pagos en un periodo definido por cuenta IBAN. e. Emisión de comprobantes individualizados de pago Máximo
RF-SUPRES.14	**Consultas Generales y específicas por institución**. Según el usuario y el perfil correspondiente, el sistema debe prever consultas para todas las instituciones por cada una de las incluidas en el sistema, programas sociales y beneficios, permitiendo filtrar por cada uno de sus atributos. Las consultas deben poder exportarse a herramientas ofimáticas
RF-SUPRES.15	**Facilidades de Exportación.** El sistema debe brindar a los usuarios, mecanismos que les permitan exportar los distintos informes generados por la aplicación a documentos de texto en formato legibles por herramientas ofimáticas y, cuando se requiera, como planillas de cálculo. Esta funcionalidad debe ser configurable en cuanto a la forma en que se desea. Todos los reportes deben proporcionar información en tiempo real.
RF-SUPRES.16	**Estructura de los reportes.** Los reportes deben tener dos áreas diferenciadas: (i) El área de filtros; y (ii) Un área de resultados donde aparecerá la tabla con el conjunto de registros que satisfagan los filtros de búsqueda. El área de filtros presentará por defecto la búsqueda simple, que ofrecerá un conjunto de filtros reducido y de uso común. Debe ofrecer la posibilidad de pasar a búsqueda avanzada, que desplegará bajo el área de filtros básicos un conjunto de filtros adicionales de uso más específico.
RF-SUPRES.17	**Seguridad:** El sistema debe poder discriminar el acceso a las diferentes funcionalidades según los perfiles y roles que se establezcan en el módulo que administre la seguridad, de acceso y los roles y perfiles. Se prevé que el ingreso al sistema únicamente se controle mediante el uso de firma digital, consumiendo el firmador del Banco Central de Costa Rica y que por lo tanto sea multi navegador, para que pueda ser accesado sin restricción, con sus respectivas bitácoras, conforme la definición que al efecto se establezca.

7. REQUERIMIENTOS NO FUNCIONALES

7.1 Requerimientos Generales del Servicio de Implementación

RNF- RGS	Requerimientos Generales del Servicio de Implementación
RNF-RGS.01	El oferente deberá realizar la consultoría en un plazo máximo de 22 meses calendario (8 meses de implementación, 2 meses de estabilización y 12 meses de mantenimiento evolutivo), a partir de la orden de inicio.
RNF-RGS.02	La consultoría, para efectos de coordinación, supervisión y presentación de productos, deberá trabajar con el personal designado como contraparte por Tesorería Nacional y de Tecnologías de Información y Comunicación (DTIC); así como con la Unidad Coordinadora del Proyecto Hacienda Digital (UCP).
RNF-RGS.03	La consultoría deberá priorizar el trabajo remoto, siempre que sea posible. Al inicio del proyecto y durante su ejecución, se acordarán las tareas a desarrollar en forma remota y presencial. El trabajo que se realice de manera remota y en forma conjunta con personal del Ministerio de Hacienda, deberá realizarse con un mínimo de seis horas de coincidencia con los horarios de trabajo habituales del Ministerio de Hacienda en Costa Rica.
RNF-RGS.04	El oferente deberá llevar a cabo la consultoría en sus propias oficinas. El Ministerio de Hacienda dispondrá de salas de reuniones y oficinas para las tareas que se realicen en forma presencial, previa coordinación y mutuo acuerdo.
RNF-RGS.05	El oferente debe entregar al MdH la configuración detallada de arquitectura requerida por la solución ofertada. Incluye la lista de todos los recursos y licenciamientos, con sus respectivos dimensionamientos. Debe especificar el esquema de comunicaciones y redes, entre otros elementos según lo indicado en el Diseño de Infraestructura.
RNF-RGS.06	La solución ofertada deberá instalarse en diferentes ambientes (entornos) de desarrollo, calidad, homologación y producción según corresponda.

7.2 Requerimientos de Metodología.

RNF-MET	Requerimientos metodológicos
RNF-MET.01	La firma consultora debe incluir mecanismos de colaboración y comunicación permanente con el Ministerio de Hacienda y los involucrados para la revisión de los avances y la toma de decisiones del Proyecto.
RNF-MET.02	La firma consultora debe trabajar en conjunto con el Ministerio en la definición y el establecimiento de un modelo de gobernanza del proyecto que permita coordinar las partes involucradas y tomar las decisiones relacionadas con el desarrollo de los entregables de manera efectiva, transparente y eficiente.
RNF-MET.03	El modelo de gobernanza del proyecto debe contemplar como mínimo los siguientes aspectos: • Definición de un patrocinador del proyecto. • Identificación de las partes involucradas en el proyecto, con cargos, nombres y datos de contacto de las personas. • Definición de los roles y responsabilidades de cada una de las partes involucradas en el servicio.
RNF-MET.04	La firma consultora deberá aplicar una metodología ágil para el desarrollo y mantenimiento del software de este proyecto, la cual debe estar apegada a los principios del Manifiesto Ágil (https://agilemanifesto.org/iso/es/principles.html).
RNF-MET.05	El oferente deberá definir los formatos y procedimientos para la gestión del Proyecto. Entre otros: • Formato de plan de trabajo. • Formato de actas de reuniones de seguimiento. • Formato de reporte quincenal con el estado y avance del Proyecto. • Formato de reporte mensual con el cumplimiento de las actividades, tareas y entregables previstos para el periodo. • Formato de gestión de cambios. • Formato de aceptación de entregables. • Formato de aceptación de hitos de pago.
RNF-MET.06	Entregar todos los documentos que hacen parte del contrato y del proyecto en idioma español.
RNF-MET.07	El análisis de riesgos debe incluir los riesgos y su estrategia de mitigación como mínimo. Se debe presentar con la propuesta un análisis inicial (línea base) de los riesgos y estrategia de mitigación. Debe incluir procedimientos que garanticen que las acciones de mitigación se realizarán.
RNF-MET.08	Se debe presentar la metodología para gestionar cambios en el proyecto, con cargo a la bolsa de horas: el procedimiento, los roles que intervienen, los tiempos, metodologías que permitan verificar en detalle la evaluación de costos de los cambios.
RNF-MET.09	Incorporar en los entregables la retroalimentación y las recomendaciones del Ministerio de Hacienda.

RNF-MET	Requerimientos metodológicos
RNF-MET.10	Tomar acciones basado en los resultados de los indicadores clave de avance del Proyecto.
RNF-MET.11 RNF-MET.12	Realizar la transferencia de conocimiento permanentemente al equipo contraparte del Ministerio de Hacienda en cada una de las etapas de Proyecto. Cualquier documento que la firma consultora presente ante el MdH, sea de un informe o un entregable, debe contar con una presentación adecuada, incluyendo al menos portada, índice, numeración de páginas, logos del MdH, entrega en formato digital Word y PDF y firma de la persona(s) responsable(s) de la firma consultora. En caso de incumplimiento, el documento no será aceptado por parte del MdH.

7.3 Requerimientos de Planificación.

RNF-PLA	Requerimiento
RNF-PLA.01	Para la gestión general del proyecto la firma consultora deberá presentar un Plan de Trabajo detallado, elaborado con base en las prácticas definidas en el PMBOK y que cubra los siguientes temas: • Alcance Detallado • Plan de recursos • Plan de riesgos • Plan de calidad • Plan de verificación • Plan de comunicación • Cronograma de implementación y entregables (WBS) • Plan de seguimiento y evaluación • Plan de capacitación • Proceso de control de cambios
RNF-PLA.02	El Plan de Trabajo presentado por la firma consultora debe incluir un cronograma detallado del proyecto, el cual debe estar en formato MS Project y Excel, y en el cual debe incluir todas las actividades necesarias para cumplir con el alcance del proyecto, agrupándolas en diferentes niveles de detalle, con sus respectivos tiempos, recursos, especificando hitos, responsables-equipos y con referencia a los requerimientos. Este cronograma debe definir los roles de la organización del proyecto y demás participantes del proyecto. El nivel de granularidad debe ser de semanas.

RNF-PLA	Requerimiento
RNF-PLA.03	La firma consultora debe participar en las actividades necesarias para entendimiento del alcance y cumplimiento del objeto del contrato. Incluye entre otras tareas: • Participar en las reuniones de entendimiento del alcance del proyecto con el Ministerio de Hacienda y las partes interesadas en el proyecto. • Preparar y realizar la reunión de lanzamiento de Proyecto (*kick-off meeting*). • Entregar la presentación y el informe de la reunión de lanzamiento de Proyecto.
RNF-PLA.04	La firma consultora debe utilizar la herramienta de proyectos automatizada que facilite el seguimiento al cronograma, actividades y entregables del proyecto. Todas las herramientas que se usen para gestionar el proyecto deben permitir acceso a funcionarios del Ministerio de Hacienda, con permisos adecuados.
RNF-PLA.05	En lo referente al desarrollo del software, la firma consultora deberá utilizar una metodología ágil, aplicando de manera correcta los principios, etapas, ceremonias y eventos enunciados en la metodología propuesta, conformando un equipo de trabajo que incluya los roles requeridos.
RNF-PLA.06	La firma consultora deberá incluir en el equipo de trabajo un representante del negocio, el cual será designado por el MdH.
RNF-PLA.07	La firma consultora deberá apoyar al representante del negocio designado por el MdH en sus diferentes tareas, ofreciéndole asesoramiento en el cumplimiento del rol que le corresponde en la metodología ágil propuesta y de esta manera el proceso ágil se desarrolle sin contratiempos.
RNF-PLA.08	La firma consultora deberá atender durante el proceso de desarrollo las definiciones y priorizaciones que realice el representante del negocio, de forma tal que se asegure que la solución desarrollada genera el mayor valor posible para el Ministerio de Hacienda.
RNF-PLA.09	El equipo de desarrollo deberá elaborar la lista de riesgos del proyecto y el cronograma del proyecto, manteniendo ambos instrumentos actualizados a lo largo del proyecto.
RNF-PLA.10	El desarrollo del producto deberá ser realizado de manera incremental, por medio de la ejecución de ciclos cortos de desarrollo, para lo cual existirá una planificación de los compromisos y entregables que será cumplidos por parte del equipo de desarrollo en cada ciclo.
RNF-PLA.11	El representante del negocio designado por el MdH será el responsable de emitir el criterio de aceptación sobre el producto desarrollado a lo largo de los diferentes ciclos cortos de desarrollo.

RNF-PLA	Requerimiento
RNF-PLA.12	La metodología ágil propuesta deberá contar con los instrumentos que permitan conocer de manera clara y transparente el avance alcanzado y el trabajo pendiente para cumplir con la finalización de la solución requerida.
RNF-PLA.13	La aceptación del software desarrollado será dada por parte del MdH a partir del cumplimiento satisfactorio del producto esperado, alcanzado a su vez a través de la aceptación a satisfacción de los criterios de aceptación y terminado de los entregables logrados en los ciclos cortos de desarrollo ejecutados.
RNF-PLA.14	En caso de que la firma consultora se atrase en más de 10 días hábiles en la entrega de la solución, según cronograma detallado del proyecto, (por razones imputables al contratista), el Contratante, le impondrá una multa por cada día hábil de atraso adicional en la entrega, cuyo importe corresponderá a un 0.25% del precio del contrato.

7.4 Requerimientos para garantizar la portabilidad de aplicaciones desarrolladas en Nube.

ID	Descripción
RNF-POR.01	La firma consultora debe garantizar que las aplicaciones que desarrolle para el Ministerio de Hacienda serán portables a diferentes entornos, sea de nube u otro tipo, sin requerir su reescritura, debiendo funcionar de manera transparente en el nuevo entorno y sin tener dependencias en servicios del entorno de operación anterior. Para ello deberá incluir como parte de las pruebas de entrega y aceptación, pruebas de portabilidad a otros ambientes.
RNF-POR.02	La firma consultora debe garantizar que las aplicaciones que desarrolle para el Ministerio de Hacienda funcionarán de manera óptima en cualquiera de las nubes que aparecen en el cuadrante de Líderes en servicios de infraestructura y plataforma, según el último estudio de Gartner, en modalidad IaaS o máquinas virtuales.
RNF-POR.03	La aplicación debe ser diseñada en una arquitectura de microservicios y serverless, dividiendo la funcionalidad en componentes independientes, los cuales deben ser autónomos y desplegables de manera independiente unos de otros. Cuando no apliquen estos conceptos de arquitectura se deberán justificar y ser aprobados por el MdH.
RNF-POR.04	La interacción entre los microservicios debe ser implementada cumpliendo con el estándar de la arquitectura, esto es, a través de la exposición de APIs (Application Program Interfaces).
RNF-POR.05	La aplicación debe ser desarrollada utilizando estándares abiertos y herramientas software libre que operen en diversos ambientes de nube o

	fuera de ellas, evitando la dependencia sobre productos propietarios a un ambiente particular.
RNF-POR.06	La aplicación debe ser desarrollada utilizando Docker como plataforma de contenedorización, para el empaquetamiento de los componentes y dependencias en la forma de contenedores, los cuales deben poder ser ejecutados en cualquier entorno, aislándolos del sistema operativo y servidor, posibilitando su portabilidad entre diferentes entornos.
RNF-POR.07	La aplicación desarrollada debe utilizar Kubernetes para la administración del despliegue, ejecución y gestión de los contenedores de manera eficiente, garantizando su portabilidad.
RNF-POR.08	La firma consultora deberá utilizar servicios de nube que garanticen la portabilidad entre diferentes entornos para las diferentes necesidades de la aplicación tales como la contenedorización, ejecución de las aplicaciones, procesos de analítica, gestión de las bases de datos, extracción de datos, machine learning, almacenamiento de objetos, despliegue continuo, entre otros.
RNF-POR.09	La nube a utilizar debe contar con una estrategia de “nube abierta” que facilite la migración de aplicaciones a distintas ubicaciones y nubes.
RNF-POR.10	La nube a utilizar debe cumplir con el estándar CDMI (Cloud Data Management Interface) para facilitar a las aplicaciones crear, recuperar, actualizar y eliminar elementos de datos del almacenamiento en la nube.
RNF-POR.11	La nube a utilizar debe contar con herramientas y servicios que faciliten la migración de grandes conjuntos de datos.
RNF-POR.12	La firma consultora deberá someter a aprobación del MdH las decisiones de arquitectura y herramientas que serán utilizadas para el desarrollo de manera previa a la implementación.

7.5 Requerimientos del proceso de desarrollo de aplicaciones en Nube.

ID	Descripción
RNF-DES.01	La firma consultora debe configurar para el desarrollo de software diferentes ambientes (entornos) de desarrollo, calidad, homologación y producción.
RNF-DES.02	La firma consultora debe certificar que los entornos de desarrollo, calidad, homologación y producción cumplen con los requerimientos de seguridad, capacidad y configuración requeridos para operar de acuerdo con las condiciones definidas en este documento.
RNF-DES.03	La firma consultora debe aplicar en el desarrollo de software patrones de diseño que permitan que sus componentes funcionen en capas de tal forma que las capas superiores llamen a las inferiores, nunca las inferiores a las

	superiores, y diferencie por lo menos la capa de interfaz de usuario o front-end, la capa de negocio y servicios, la capa de (acceso a) datos, y la capa de los repositorios de datos. Debe implementarse seguridad en todas las capas.
RNF-DES.04	La firma consultora debe garantizar que los componentes de software desarrollados podrán ser monitoreados, que cumplirán con los requerimientos de seguridad de control de acceso y de autenticación.
RNF-DES.05	La firma consultora debe configurar un entorno de desarrollo integrado (IDE) para el desarrollo los componentes de software.
RNF-DES.06	La firma consultora debe implementar mecanismos en el ambiente de desarrollo de software donde se proteja al usuario de la ejecución involuntaria de operaciones que puedan generar fuertes impactos en el negocio (por ejemplo, exigiendo confirmar deshabilitaciones de servicios, borrados de servicios, borrados de información).
RNF-DES.07	La firma consultora debe asegurar que todas las transacciones con actualizaciones sean atómicas y deben permitir recuperar el estado de los datos al comienzo de la ejecución de la transacción en el evento de que ocurran fallas antes de finalizar (o de hacer un “commit”).
RNF-DES.08	La firma consultora debe contar con una herramienta para el control de versiones en los desarrollos de software que se realicen durante la vida del contrato. Dicha herramienta deberá ser compatible con herramientas de control de versiones (SVN, GIT u otro).
RNF-DES.09	La firma consultora debe ofrecer un ambiente de colaboración para los equipos desarrolladores de los componentes de software.
RNF-DES.10	La firma consultora debe documentar internamente el código fuente de los desarrollos realizados cumpliendo con los estándares que defina el MdH.
RNF-DES.11	La firma consultora debe entregar al MdH el código fuente de los desarrollos realizados, para todas las versiones generadas.
RNF-DES.12	La firma consultora debe contar con una herramienta de desarrollo que permita la construcción, pruebas y depuración de forma nativa de los componentes de software desarrollados por medio de una interfaz gráfica (GUI).
RNF-DES.13	La firma consultora debe utilizar técnicas de diseño y lenguajes orientados a objetos para el desarrollo de los componentes de software y cumplir con los 5 principios SOLID del diseño orientado a objetos • S: (Single) Principio de responsabilidad única. • O: (Open) Principio abierto-cerrado. • L: (Liskov) Principio de sustitución de Liskov.

	• I: (Interface) Principio de segregación de interfaz. • D: (Dependency) Principio de inversión de dependencia.
RNF-DES.14	La firma consultora debe incluir en los componentes de software desarrollados información visual al usuario sobre el avance progresivo cuando se estén ejecutando procesos complejos demorados (por ejemplo: barras de progreso u otro tipo de aviso en un proceso batch, en una búsqueda larga, en la generación de un reporte largo).
RNF-DES.15	La firma consultora debe incluir en los componentes de software desarrollados mensajes de error claros, comprensibles, codificados y que guíen al usuario sobre qué hacer para corregir la situación de error.
RNF-DES.16	La firma consultora debe cumplir en los componentes de software desarrollados, cuando se trate de interacción con el usuario, lo siguiente: a) Ayuda sensible al contexto para ventanas y campos de ingreso de información (hints o micro-ayudas) donde se requiera. b) Cumplimiento de las regulaciones para personas con discapacidad en concordancia con lo indicado en el nivel de conformidad AAA de la *Directriz Implementación de Sitios Web Accesibles en el Sector Público Costarricense*. c) Menús personalizados según el perfil del usuario que ingresa. d) La solución debe mostrar al usuario, su ruta o ubicación lógica de acuerdo con el contexto (por ejemplo, mediante “breadcrumbs” u otra forma).
RNF-DES.17	La firma consultora debe cumplir en los componentes de software desarrollados, cuando estos desplieguen resultados al usuario, con la segmentación del despliegue de datos (paginar) a fin de optimizar la experiencia del usuario.
RNF-DES.18	La firma consultora debe incluir en los componentes de software desarrollados, cuando se trate de sesiones de usuario, la configuración de un plazo de timeout de inactividad de la sesión al cabo del cual la sesión deberá ser cerrada.
RNF-DES.19	La firma consultora debe utilizar sistemas administradores de bases de datos para los componentes de software desarrollados.
RNF-DES.20	La firma consultora debe entregar todos los documentos que hacen parte del contrato y del proyecto en idioma español.
RNF-DES.21	La firma consultora debe incorporar al equipo de trabajo un representante del negocio designado por el MdH.

RNF-DES.22	La firma consultora debe atender durante el proceso de desarrollo las definiciones y priorizaciones que realice el representante del negocio, de forma tal que se asegure que la solución desarrollada genera el mayor valor posible para el Ministerio de Hacienda.
RNF-DES.23	La firma consultora debe elaborar la lista de riesgos del proyecto y el cronograma del proyecto, manteniendo ambos instrumentos actualizados a lo largo del proyecto.
RNF-DES.24	La firma consultora debe realizar el desarrollo del producto de manera incremental, por medio de la ejecución de ciclos cortos de desarrollo mostrando los avances en código que se pueda ejecutar para lo cual existirá una planificación de los compromisos y entregables que será cumplidos por parte del equipo de desarrollo en cada ciclo.
RNF-DES.25	El representante del negocio designado por el MdH será el responsable de emitir el criterio de aceptación sobre el producto desarrollado a lo largo de los diferentes ciclos cortos de desarrollo.
RNF-DES.26	La metodología ágil adoptada por la firma consultora debe contar con los instrumentos y herramientas tales como estimaciones de esfuerzo de casos de uso o historias de usuario,sprint burndown chart, tableros kanban, entre otros, que permitan conocer de manera clara y transparente el avance alcanzado y el trabajo pendiente para cumplir con la finalización de la solución requerida.
RNF-DES.27	La metodología de desarrollo adoptada por la firma consultora debe ser acompañada de indicadores de avance entre los cuales debe incluir por lo menos los siguientes: 1) número de requerimientos funcionales y técnicos implementados. 2) porcentaje de implementación de cada componente del sistema, pesados los componentes según su complejidad.
RNF-DES.28	La aceptación del software desarrollado será dada por parte del MdH a partir del cumplimiento satisfactorio del producto esperado, alcanzado a su vez a través de la aceptación a satisfacción de los criterios de aceptación y terminado de los entregables logrados en los ciclos cortos de desarrollo ejecutados.
RNF-DES.29	La firma consultora debe incorporar en los entregables la retroalimentación y las recomendaciones del Ministerio de Hacienda.
RNF-DES.30	La firma consultora debe tomar acciones basado en los resultados de los indicadores clave de avance del Proyecto.
RNF-DES.31	La firma consultora debe participar en las actividades necesarias para entendimiento del alcance y cumplimiento de las necesidades a satisfacer.
RNF-DES.32	La firma consultora debe garantizar que los servicios de desarrollo de componentes de software cumplen con los criterios de aceptación por medio de la ejecución de pruebas durante el proceso de desarrollo ágil utilizado en la implementación.

RNF-DES.33	La firma consultora debe realizar la transferencia de conocimiento a la contraparte técnica del MdH en lo relacionado a instalación, gestión y monitoreo de la solución implementada, así como en lo relacionado con los componentes de software desarrollados. 1. Diseñar el plan de transferencia de conocimiento. 2. Preparar los materiales, ambientes y datos que serán requeridos durante las actividades de transferencia de conocimiento. 3. Ejecutar las actividades de transferencia de conocimiento de acuerdo con la planificación realizada. 4. Presentar un informe con los resultados de la transferencia de conocimiento y los indicadores que midan la asistencia, el conocimiento y la satisfacción del programa. El oferente debe tomar nota que la transferencia de conocimiento no debe ser considerada como servicios de capacitación. Nota: La firma consultora debe dictar las transferencias de conocimiento a la contraparte designada por el Ministerio de Hacienda de acuerdo con los lineamientos definidos sobre este tema. El MdH hará la evaluación del cumplimiento a satisfacción de los objetivos de dicha transferencia de conocimiento. En caso de que la evaluación resulte negativa, la firma consultora deberá repetir la misma, subsanando los defectos que sean identificados.
RNF-DES.34	Cuando sea requerido por parte del Ministerio de Hacienda, la firma consultora debe elaborar y entregar la documentación asociada a los desarrollos de software realizados, incluyendo documentos de requerimientos, análisis detallado, diseño detallado, manuales técnicos, de configuración, de instalación, manuales de usuario, documentos de especificaciones técnicas y funcionales. Toda la documentación deberá ser en idioma español.

7.6 Requerimientos de Pruebas.

RNF-PRU-01	Requerimientos de Pruebas
RNF-PRU.01	La firma consultora debe garantizar que la solución desarrollada cumple con los criterios de aceptación por medio de la ejecución de pruebas durante el proceso de desarrollo ágil utilizado en la fase de implementación.

RNF-PRU-01	Requerimientos de Pruebas
RNF-PRU.02	La firma consultora deberá incluir en la planificación de los diferentes ciclos cortos de desarrollo, la realización de las pruebas que serán aplicadas sobre los entregables desarrollados, detallando la forma en que serán realizadas.
RNF-PRU.03	Los criterios de aceptación de los entregables deberán incluir la conclusión a satisfacción de las pruebas de calidad de los entregables desarrollados.
RNF-PRU.04	Las pruebas de calidad de los entregables desarrollados deberán incluir tanto pruebas funcionales como técnicas y de seguridad.
RNF-PRU.05	La firma consultora deberá preparar los datos de prueba, entornos y parametrizaciones necesarias para la ejecución de las pruebas, así como coordinar con las contrapartes requeridas del MdH y entes externos para la ejecución de las pruebas.
RNF-PRU.06	La firma consultora deberá calendarizar la realización de las pruebas integrales (pruebas de procesos de comienzo a fin), pruebas de rendimiento (carga y estrés), pruebas de respaldo y recuperación cuando el cronograma de lanzamiento de la solución así lo requiera.
RNF-PRU.07	La firma consultora deberá aplicar pruebas de regresión de preferencia automatizadas cada vez que realice cambios sobre entregables previamente aceptados.
RNF-PRU.08	La firma consultora debe solucionar los defectos identificados hasta dar cumplimiento a los criterios de aceptación para la salida a producción.
RNF-PRU.09	La firma consultora debe, al finalizar las pruebas los componentes de software desarrollados, presentar los informes de resultados.

7.7 Atención de Incidentes

RNF- SER	Atención de Incidentes
RNF-SER.01	El soporte técnico para la atención de incidentes por parte de la firma consultora, estará disponible de 7am a 8pm de lunes a viernes, en caso de imprevistos según la coordinación respectiva.
RNF-SER.02	La firma consultora debe ofrecer un esquema de soporte conformado por los siguientes canales de atención, recursos de soporte y características: • Línea telefónica fija o celular (móvil) con disponibilidad requerida según requerimiento RNF-SER.01, con atención en idioma español.

<table>
<tr><td></td><td>

- Correo electrónico atendido en idioma español o inglés.

</td></tr>
<tr><td>RNF-SER.03</td><td>La firma consultora pondrá a disposición del Contratante, el software que permita registrar las incidencias relacionadas con errores de la plataforma, así como contar con una dirección de correo electrónico y un número de teléfono fijo y móvil, para que el Contratante reporte las incidencias.</td></tr>
<tr><td>RNF-SER.04</td><td>El Ministerio de Hacienda puede crear un número ilimitado de solicitudes de atención producto de incidencias sucedidas en el funcionamiento de la solución posterior a la salida a producción y estas deben ser entendidos y atendidos de la siguiente manera.

Severidad de los incidentes

La siguiente tabla define la severidad de los incidentes:

<table>
<tr><th>Severidad incidente</th><th>Definición</th></tr>
<tr><td>Grave</td><td>Indisponibilidad total en el entorno de producción, o pérdida de funcionalidad en un “componente crítico” sin solución alterna.</td></tr>
<tr><td>Media</td><td>Pérdida de un “componente crítico” pero existe una solución alternativa, o indisponibilidad de un “componente importante” sin solución alterna.</td></tr>
<tr><td>Baja</td><td>Disminución en la funcionalidad o el rendimiento, sin embargo, la Solución aún funciona según lo especificado.</td></tr>
</table>
</td></tr>
<tr><td>RNF-SER.05</td><td>La firma consultora dispondrá de los siguientes niveles de servicio en función de la gravedad de la incidencia reportada por el contratante:

<table>
<tr><td></td><td>Grave</td><td>Media</td><td>Baja</td></tr>
<tr><td>Tiempo de Respuesta</td><td>30 minutos</td><td>2 horas</td><td>4 horas</td></tr>
<tr><td>Tiempo de Resolución</td><td>1 hora</td><td>4 horas</td><td>8 horas</td></tr>
</table>

Notas

- Los tiempos de respuesta y resolución, los períodos de tiempo indicados corren a partir de que se reporta el evento.
- En todos los casos, los plazos contarán indistintamente de que los eventos ocurran en días u horas hábiles o inhábiles.
- En caso de que el Consultor o Firma incumpla con los tiempos de respuesta y/o de resolución de los incidentes, el Contratante le impondrá una multa cuyo importe corresponderá a un 0.04%

</td></tr>
</table>

	del monto del contrato por cada hora de retraso en la resolución del incidente. El monto de la multa deberá ser cancelado por la firma consultora dentro de los diez días posteriores a su firmeza. En caso de no ser cancelado, será aplicado a la garantía de cumplimiento rendida por la firma consultora para este fin,
RNF-SER.06	La firma consultora deberá presentar un informe mensual de incidencias ocurridas, tiempos de respuesta y tiempos de resolución.
RNF-SER.07	La firma consultora creará un registro de las incidencias y de la resolución de cada una de ellas que contendrá lo siguiente: - Descripción detallada del problema, su causa y el detalle de la solución realizada. - Personal asignado para la resolución de éste. - Problemas presentados durante la resolución. - Documentación adjunta que sustente los cambios hechos (procedimientos, documentación, etc.). - Recomendaciones. - Fecha y hora de la recepción - Fecha y hora de resolución
RNF-SER.08	Para el control y registro de las incidencias, solicitudes de mantenimiento, cambios, incidentes, problemas y soporte durante la vigencia del contrato y durante el período de soporte y mantenimiento, se utilizará la Herramienta de Gestión del Servicio (ITSM) del MdH, la cual tendrá parametrizados los niveles de servicio solicitados por el Ministerio de Hacienda.

7.8 Estabilización

RNF- MON	**Monitoreo**
RNF-EST.01	La firma consultora deberá monitorear el desempeño del sistema, durante la Fase de Estabilización. El principal objetivo de esta fase será atender y corregir cualquier problema de funcionamiento que se presente durante los primeros dos meses a partir de la puesta en operación del Sistema con un soporte remoto o in-situ cuando sea requerido por el Ministerio de Hacienda.

7.9 Mantenimiento evolutivo de ajustes, actualizaciones y mejoras

RNF- MAN	Mantenimiento evolutivo de ajustes, actualizaciones y mejoras
RNF-MAN.01	La firma consultora deberá prestar servicios para realizar el mantenimiento evolutivo de la solución, durante la cual el MdH podrá solicitar la implementación y documentación de mejoras o ampliaciones a las funcionalidades del Sistema una vez puesto en operación. Para los fines indicados, se establece una Bolsa de 500 horas que será utilizada a entera discreción del Ministerio de Hacienda. No existe obligación del Ministerio de Hacienda de utilizar un determinado número de horas.
RNF-MAN.02	De manera previa al desarrollo de requerimientos de mantenimiento evolutivo a las funcionalidades del Sistema, el Consultor debe presentar para visto bueno del Ministerio, el cronograma de actividades y la cantidad de horas de trabajo de cada consultor requerido para llevar a cabo la nueva evolución o mejora.
RNF-MAN.03	Los servicios cargados a la Bolsa de Horas deberán contar con la aprobación técnica y funcional del Ministerio de Hacienda para su pago.
RNF-MAN.04	Una vez la solución sea aceptada por el Ministerio de Hacienda y la solución se encuentre desplegada en el ambiente de producción la firma consultora debe brindar el servicio de mantenimiento evolutivo con cargo a la bolsa de horas, cumpliendo con los siguientes lineamientos. Las solicitudes y tickets de mantenimiento evolutivo se documentarán, registrarán y pondrán a disposición para su respectivo análisis y evaluación por parte del consultor. Cada solicitud constará al menos de la siguiente información: • Objeto (componente de software); • Funcionalidad sobre la cual se desea hacer la solicitud de mantenimiento evolutivo; • Explicación del requerimiento; • Nombre de la persona que solicita; • Número de teléfono y dirección de correo electrónico para el contacto;
RNF-MAN.05	El consultor debe atender las solicitudes de mantenimiento evolutivo dentro de los siguientes tiempos: - Estimación: 5 días hábiles como máximo. - Implementación: Según lo acordado entre las partes de acuerdo con la complejidad del requerimiento y las necesidades del Ministerio de Hacienda.
RNF-MAN.06	La firma consultora debe establecer el procedimiento para que los usuarios puedan crear las solicitudes de mantenimiento evolutivo.

RNF-MAN.07	La firma consultora brindará los servicios de mantenimiento evolutivo en idioma español y con disponibilidad dentro del horario hábil del MdH.
RNF-MAN.08	A partir de los mantenimientos evolutivos implementados sobre la solución, la firma consultora debe actualizar la lista de preguntas frecuentes identificadas a lo largo de la prestación del servicio de soporte y la base de conocimiento relacionada con la solución.
RNF-MAN.09	La firma consultora debe realizar los despliegues de los mantenimientos evolutivos en los ambientes de calidad y homologación y debe prestar soporte al personal que el Ministerio de Hacienda designe en los despliegues en el ambiente de producción.
RNF-MAN.10	La firma consultora debe realizar pruebas de regresión en cada uno de los despliegues con el fin de garantizar que los cambios no afecten el correcto funcionamiento de las funcionalidades existentes.
RNF-MAN.11	La firma consultora debe actualizar la documentación técnica y funcional de los mantenimientos evolutivos implementados. Además, debe entregar las guías, protocolos y manuales de instalación requeridos en el despliegue de los mantenimientos evolutivos en producción y realizar la capacitación y transferencia de conocimiento a los encargados por parte del MdH
RNF-MAN.12	En caso de que la firma consultora incumpla en más de 5 días hábiles con los tiempos acordados para implementación de la mejora, el Contratante le impondrá una multa cuyo importe corresponderá a un 5% del monto acordado por la mejora por cada día hábil de retraso en la entrega.

7.10 Migración de datos

La migración de los datos es uno de los mayores retos en el proceso de implementación, a la vez que abre una ventana de oportunidades para evaluar y mejorar la calidad de la información disponible. La responsabilidad de la calidad de los datos es del MdH, sin embargo, la responsabilidad de mover, transformar y cargar los mismos en el nuevo sistema, y de identificar nuevos datos necesarios, son del contratista.
Internamente el Ministerio está realizando tareas de inventario, análisis y mejoramiento de la calidad de los datos y la data a migrar propiedad del negocio (MH).
Se espera que la firma consultora realice como mínimo las siguientes etapas (proponiendo y usando su propia metodología y herramientas):

- Análisis de brechas. En esta fase se conoce en detalle lo que hizo el Ministerio. Se compara lo que se tiene con lo que se necesita en la nueva solución, determinando las brechas.

- Diseño y programación de la migración. Con base en lo que entregará el Ministerio y lo que requiere el nuevo sistema, el contratista deberá planear y diseñar todos los pasos de la migración.
- Ejecución de Programas. Es la ejecución de los programas diseñados para la migración.
- Pruebas Técnicas y funcionales. Son las pruebas para verificar que el proceso de migración se realizó correctamente.

RNF-MIG	**Requerimientos de Migración de Datos de SUPRES**
RNF-MIG-01	La firma consultora debe realizar un Plan de Migración de Datos basado en las actividades realizadas por el MdH y las necesidades específicas de datos de la solución. Cualquier desviación o cambio deberá ser consultado y aprobado por el MdH.
RNF-MIG-02	La firma consultora debe construir los procesos de extracción, transformación, y carga de los datos para llevar a cabo la migración.
RNF-MIG-03	La firma consultora en conjunto con el MH coordinará con las unidades que correspondan, realizará la extracción, transformación, y carga de datos a partir de los sistemas y las fuentes de datos identificados en el Plan de Migración de Datos.
RNF-MIG-04	La firma consultora debe desarrollar, configurar o ajustar los programas de conversión y migración según se requiera. En caso alguna información no se encuentre sistematizada, el oferente deberá proveer la plantilla de carga de la información para ser llenada por funcionarios del Ministerio de Hacienda. La firma consultora debe probar los procesos de conversión y migración en los sprints según los datos que se requieran en el ambiente que se determine para este fin.
RNF-MIG-05	La firma consultora debe ejecutar los procesos de conversión y migración definitivos para el ambiente de producción y certificación. Los mismos deberán ejecutarse tantas veces como se requiera de acuerdo con las fases y lanzamientos que se definan en el cronograma del proyecto.
RNF-MIG-06	La firma consultora debe construir procedimientos de validación de los datos migrados a la solución, de tal manera que sea posible garantizar y certificar que los datos han sido migrados sin ningún tipo de alteración.

RNF-MIG-07	La firma consultora debe ejecutar las validaciones de los datos convertidos y migrados. Este proceso debe realizarse de forma conjunta con funcionarios del Ministerio de Hacienda, quienes deberán certificar los niveles de calidad de los datos y aprobarán o no el resultado obtenido. La responsabilidad de la calidad de los datos es del MdH, pero la mecánica de extracción, transformación y cargue de los datos al nuevo sistema es del contratista.
RNF-MIG-08	La firma consultora debe realizar pruebas de los datos migrados a la solución.
RNF-MIG-09	La firma consultora debe presentar el reporte de seguimiento a la información rechazada en el proceso de migración de datos que contenga como mínimo: • Registros migrados • Errores detectados • Tiempo de ejecución de los procesos • Categoría de los rechazos • Análisis causa raíz • Decisiones acerca de los rechazos
RNF-MIG-10	La firma consultora junto con la empresa que da mantenimiento a Tesoro Digital, debe realizar la extracción, transformación, y carga de datos de: • Beneficiario (identificación, sexo, nombre, correo electrónico, teléfono, escolaridad, división política). • Destinatario (identificación, sexo, nombre, correo electrónico, teléfono, escolaridad, división política). • Tipo de Identificación (cédula identidad/DIMEX/DIDI/Gobierno/Jurídico/Institución Autónoma). • Institución • Programa de cada institución • Monto del beneficio • Fecha de la Transacción-Pago (Desde/Hasta)

	• Periodo (Anual/Mensual/Semanal)-Gráficos • Estado de la Transacción (Aprobado o Rechazado) • Cuentas IBAN (Beneficiario/Destinatario)

7.11 Capacitación

La firma consultora debe incluir en su oferta un programa formal de capacitación al personal del Ministerio de Hacienda en todo lo relacionado con el sistema desarrollado a nivel de operación (usuario final), a nivel de administración de sistema, instalación y a nivel de desarrollo de la solución. El programa de capacitación no podrá ser menor a las 16 horas, deberá estar dirigido al personal que el MdH indique. Deberá realizarse una evaluación de conocimientos al finalizar la misma. Debe incluir un manual detallado para el usuario en versión digital.

RNF- CAP	Capacitación.
RNF-CAP.01	La firma consultora debe brindar capacitación sobre las metodologías estructurada y ágil que serán aplicadas durante el proyecto al equipo contraparte e interesados (stakeholders), detallando los roles y responsabilidades de cada miembro del equipo de proyecto.
RNF-CAP.02	La firma consultora debe brindar capacitación de usuario final a 8 funcionarios del Ministerio de Hacienda en el uso de la plataforma desarrollada.
RNF-CAP.03	La firma consultora debe brindar capacitación de administradores de la plataforma a 5 funcionarios del Ministerio de Hacienda a fin de que puedan realizar las tareas de parametrización, instalación, administración y respaldos de la solución.
RNF-CAP.04	La firma consultora debe brindar capacitación y transferencia de conocimiento para el mantenimiento futuro de la solución desarrollada a 10 funcionarios del Ministerio de Hacienda.
RNF-CAP.05	La firma consultora debe capacitar al funcionario del Ministerio de Hacienda que desempeñará la función de Representante del Negocio.

7.12 Requerimientos Tecnológicos Generales

RNF-TEC	Requerimientos tecnológicos
RNF-TEC-.01	SUPRES deberá integrarse con el Tesoro Digital y CGP para el intercambio de información. Para la integración se debe utilizar API.
RNF-TEC-.02	Todo el código de desarrollo debe ser documentado y entregado a la administración para su futuro soporte y mantenimiento.
RNF-TEC-.03	La empresa adjudicataria deberá desarrollar todas las interfases necesarias para la interacción con los sistemas que se integraran, a saber, Tesoro Digital - SIGAF así como CGP y solución Financiera que se adjudique en el contexto del proyecto de HD.
RNF-TEC-.04	Todas las consultas deben ser en tiempo real y contra la información o base de datos de los sistemas.
RNF-TEC-.05	Las solicitudes de pago deben permitir cargar la información de archivos de múltiples líneas, este formato debe ser definido y publicado dentro del mismo sitio. La carga del archivo debe aplicar las validaciones sobre el contenido de manera previa a la aceptación del archivo.

7.13 Arquitectura tecnológica

RNF-ARQ	Requerimientos de Arquitectura Tecnológica
RNF-ARQ.01	El sistema debe ser desarrollado en una arquitectura 100% web.
RNF-ARQ.02	La solución debe usar paquetes de bases de datos relacionales ampliamente usados en el mercado. Si es un paquete open source debe tener soporte empresarial.
RNF-ARQ.03	La solución debe estructurarse en capas de tal forma que las capas superiores llamen a las inferiores, nunca las inferiores a las superiores, y diferencie por lo menos la capa de interfaz de usuario o front-end, la capa de negocio y servicios, la capa de (acceso a) datos, y la capa de los repositorios de datos. Debe implementarse seguridad en todas las capas.
RNF-ARQ.04	El desarrollo de la solución debe utilizar microservicios y contenedores.
RNF-ARQ.05	La solución debe contar con una arquitectura SOA *(Arquitectura Orientada a Servicios)* para la integración con las plataformas externas.
RNF-ARQ.06	La integración con plataformas externas a la solución deberá realizarse mediante APIs, siguiendo principios de arquitectura y protocolos estándares de la industria (**REST** *(es una interfaz para conectar varios sistemas basados en el protocolo HTTP),* **SOAP** *(es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML)*), aplicando los mecanismos de

	seguridad (autenticación, control de acceso) definidos en el apartado de Seguridad de la Información.
RNF-ARQ.07	El desarrollo debe ser realizado con lenguajes orientados a objetos, utilizando técnicas de diseño y buenas prácticas de desarrollo en lenguajes orientados a objetos.
RNF-ARQ.08	Para el desarrollo de las interfaces y capas de presentación deben utilizarse frameworks de lenguajes de scripting (como JavaScript, Angular, React, o equivalentes)
RNF-ARQ.09	La firma consultora debe elaborar un diccionario de datos de la base de datos de la solución, compuesto de las diversas entidades que componen la base de datos, junto con la descripción de tablas, columnas, llaves primarias, índices, vistas, procedimientos almacenados, triggers.

7.14 Experiencia de usuario

RNF-UX	Requerimientos de Experiencia de Usuario
RNF-UX.01	El sistema debe permitir incorporar ayudas en línea interactivas que incluyan: a. Ayuda de contexto para ventanas y campos de ingreso de información (hints o micro-ayudas) donde se requiera. b. Ayuda en línea con acceso contextual por ventana.
RNF-UX.02	Debe generar mensajes de error claros, comprensibles, codificados y que guíen al usuario sobre qué hacer para corregir la situación de error.
RNF-UX.03	Debe funcionar con los navegadores de mayor uso frecuente, en sus últimas dos versiones liberadas: Google Chrome, Edge, Mozilla Firefox, Apple Safari.
RNF-UX.04	La interfaz gráfica del producto se debe ajustar al diseño gráfico oficial del MdH.
RNF-UX.05	La interfaz del producto deberá estar en idioma español incluyendo los mensajes de error.
RNF-UX.06	Debe permitir que un usuario autorizado parametrice el timeout de inactividad de la sesión del usuario para cerrar su sesión.
RNF-UX.07	Se deben utilizar ayudas sensibles al contexto para ayudar a explicar, entender o visualizar mejor la interacción del sistema con el usuario.
RNF-UX.08	La solución ofrecida debe cumplir atributos de usabilidad que la califiquen aceptable para uso de la población de los diversos usuarios. La usabilidad será comprobada mediante encuestas a los diferentes grupos de usuarios (funcionarios y ciudadanos).
RNF-UX.09	La firma consultora, en el desarrollo de los componentes de software que interactúen con el usuario, debe asegurar lo siguiente:

	- Deben diseñarse bajo el enfoque de experiencia de usuario, usabilidad y accesibilidad y presentar evidencia de la implementación de estos enfoques durante el proceso de desarrollo para la solución entregada, considerando las respectivas pruebas de usuarios, incluidas personas con diferentes situaciones de discapacidad. - Incluir ayuda sensible al contexto para ventanas y campos de ingreso de información (hints o micro ayudas) donde se requiera. - Incluir menús personalizados según el perfil del usuario que ingresa. - La solución debe mostrar al usuario, su ruta o ubicación lógica de acuerdo con el contexto (por ejemplo, mediante "breadcrumbs" u otra forma). - La solución, en todos sus módulos y roles, debe cumplir con lo establecido en la norma WCAG 2.1 o versiones posteriores, en acatamiento de la directriz presidencial Número 51 MTSS-MICITT Implementación de sitios web accesibles en el sector público costarricense. - Debe alcanzar como mínimo el criterio de conformidad de nivel AA de la norma WCAG 2.1 o versiones posteriores. En casos en los que haya implementación de elementos multimedia, reautentificación, ayuda o corrección de errores, la solución debe implementar pautas y criterios del nivel AAA correspondientes, según sea el caso. - Debe evaluar la implementación de los niveles de accesibilidad correspondientes aplicando los revisores automáticos de la Metodología de Evaluación de Conformidad con la Accesibilidad en sitios Web (WCAG-EM. - Debe corregir los errores y advertencias señaladas en el informe de evaluación de los revisores automáticos antes indicados. - Deben realizar pruebas con personas usuarias con discapacidad, siguiendo la metodología de las pruebas heurísticas, convergiendo con el enfoque de usabilidad y pruebas de usuario que también debe ser implementados en la solución. Entre los usuarios participantes se deben considerar: personas con discapacidad física usuarias frecuentes de tecnologías de apoyo como: joystick o controlador por mirada, personas sordas, personas con discapacidad visual total o parcial usuarias frecuentes de lectores de pantalla y magnificadores de pantalla. Todas aquellas observaciones realizadas por las personas con discapacidad deben ser analizadas e implementadas en la versión final de la solución. - La solución debe considerar, de ser el caso, todas las normas de accesibilidad desarrolladas por el Comité Técnico CTN 03 SC 02 Accesibilidad Web, del Instituto de Normas Técnicas de Costa Rica – INTECO, las cuales puede accederse mediante el siguiente enlace: https://www.inteco.org/shop?search=accesibilidad.

	- Todas aquellas modificaciones o mantenimientos que se realicen a la solución no deben afectar, en ninguna circunstancia, los atributos ni niveles de accesibilidad requeridos en los puntos anteriores.
RNF-UX.10	El sistema debe presentar menús personalizados según el perfil del usuario que ingresa a la aplicación
RNF-UX.11	El sistema debe mostrar visualmente al usuario el avance progresivo de la ejecución de los diferentes procesos (por ejemplo: barras de progreso u otro tipo de aviso en un proceso batch, en una búsqueda larga, en la generación de un reporte largo).
RNF-UX.12	El sistema debe detectar y proteger al usuario de la ejecución involuntaria de operaciones que puedan generar fuertes impactos en el negocio (por ejemplo, exigiendo confirmar ciertos borrados de información).
RNF-UX.13	El sistema debe poder segmentar el despliegue de datos (paginar) en la interfaz de usuario usando métodos de carga parcial de información.

7.15 Parámetros y configuraciones

RNF-PAR	Requerimientos de parámetros y configuraciones
RNF-PAR-.01	El sistema desarrollado debe poderse configurar para que todas sus funciones sean en idioma español, sistema métrico decimal, utilizando mínimo 18 dígitos y 4 decimales, Específicamente, todas las tecnologías de presentación visual y el software deben ser compatibles con el conjunto de caracteres ISO IEC 8859-1
RNF-PAR-.02	El sistema debe ser capaz de generar o exportar informes en múltiples formatos (por ejemplo: hojas de cálculo, procesadores de texto, PDF y en formatos para páginas), estos formatos de generación pueden ser habilitados y deshabilitados como parte de la configuración y parametrización de la solución (por reporte, rol de usuario, o aplicación).
RNF-PAR-.03	El sistema debe permitir el envío de alertas, mensajes y notificaciones derivadas de operaciones, tales como ejecución de procesos, validaciones u otros, a través de correo electrónico, mensajes para móviles y otros canales.
RNF-PAR-.04	El sistema debe manejar el formato de fecha y hora de manera parametrizada y correspondiente a la zona horaria de Costa Rica. El sistema debe reflejar esta fecha en reportes, consultas, cálculos u otros elementos que se definan.
RNF-PAR-.05	El sistema debe permitir que distintas herramientas de reportes de terceros accedan en forma controlada a los datos almacenados.

RNF-PAR-.06	El sistema debe permitir tener en línea al menos 10 años de información sin que ello degrade el rendimiento.
RNF-PAR-.07	El sistema debe permitir el procesamiento en batch (procesamiento de grandes volúmenes de datos) incluyendo optimizaciones que mejoren el rendimiento (el throughput: velocidad a la que se transmiten los datos).
RNF-PAR-.08	El sistema debe verificar la consistencia y validez de datos que se estén cargando de fuentes externas. Si hubiera errores, se deben cargar los datos correctos y notificar los errores para su corrección. En casos donde se ponga en peligro la integridad de la información se rechazarán todos los registros.
RNF-PAR-.09	El sistema debe permitir a un usuario con los permisos adecuados, cancelar la generación de un proceso si éste está tomando demasiado tiempo u otro motivo.
RNF-PAR-.10	El sistema debe conservar la configuración, parametrización y desarrollo particular implementados, al aplicar actualizaciones de nuevas versiones, parches u otros.

7.16 Auditoría del sistema

RNF-AUDIT	Requerimientos de auditoría
RNF-AUDIT.01	El registro de auditoría debe incluir el tiempo (fecha, hora, minutos y segundos), la identificación de usuario, la identificación del sitio del usuario (IP), el código de evento, e información específica de la operación realizada.
RNF-AUDIT.02	Debe proveer mecanismos de auditoría que no afecten la operación y que su impacto en rendimiento sea mínimo.
RNF-AUDIT.03	El sistema debe garantizar la trazabilidad automática de eventos relevantes en el sistema, entre los cuales al menos: • Autenticación e identificación de usuarios/sistema • Autorización de acceso a funciones del sistema • Modificación del perfil de usuario/sistema • Consulta y modificación de datos
RNF-AUDIT.04	Debe contener reportes para análisis de los registros de auditoría que permitan realizar un análisis por fecha, por usuario, por transacciones, por tipos de datos, por sitio de acceso.
RNF-AUDIT.05	Debe incluir mecanismos que eviten cambiar o ajustar los logs para que un atacante no pueda alterarlos.
RNF-AUDIT.06	Debe permitir exportar la pista de auditoría a medios externos, sin que esto repercuta en la pista almacenada en el sistema, con medidas de seguridad como firmas digitales y mecanismos que garanticen la integridad.

RNF-AUDIT.07	Debe incluir mecanismos que permitan que excepciones como llenado del espacio del log de auditoria eviten continuar el proceso de auditoria
RNF-AUDIT.08	Debe permitir encender y apagar selectivamente la trazabilidad por diferentes criterios y tiempos (por datos, por transacciones, etc., y durante ciertas horas, días, etc.), registrando en la bitácora de auditoría la información del apagado y encendido de la trazabilidad de la auditoría.
RNF-AUDIT.09	Todas las transacciones del sistema se deben poder auditar.
RNF-AUDIT.10	Todas las operaciones de los administradores se deben auditar y no se podrán desactivar sin que sean rastreadas

7.17 Seguridad y Firma Electrónica

RNF-SEGFI	Requerimientos de seguridad
RNF-SEGFI.01	El MdH ha declarado su intención de seguimiento a los estándares de seguridad ISO/IEC 27017:2015, ISO/IEC 27018:2014, y la familia de normas INTE/ISO/IEC 27000, específicamente 27001:2013. En este sentido la firma consultora de la solución se compromete a seguir estas normas en lo que concierne al alcance de su producto y los servicios contratados.
RNF-SEGFI.02	Debe permitir controlar el acceso definiendo conjuntos de permisos y asignarlos a roles y permitiendo que los usuarios se asignen a diferentes roles.
RNF-SEGFI.03	Debe permitir que un usuario pertenezca a más de un rol a la vez.
RNF-SEGFI.04	Debe permitir que sólo los usuarios administradores creen usuarios, establezcan roles de usuarios, permisos, creen grupos y asignen roles a grupos.
RNF-SEGFI.05	Debe llevar un control detallado de los intentos fallidos y exitosos de acceso al sistema y a cada una de las opciones disponibles y el registro de alertas sobre accesos definidos como sospechosos.
RNF-SEGFI.06	El control detallado de los intentos fallidos y exitosos de acceso al sistema y a cada una de las opciones disponibles y el registro de alertas sobre accesos definidos como sospechosos, debe realizarse con base en reglas configurables.
RNF-SEGFI.07	Debe proveer herramientas u opciones que permitan el cifrado de los datos con diferentes tipos de algoritmos de llaves privadas.

RNF-SEGFI	Requerimientos de seguridad
RNF-SEGFI.08	Debe permitir transmitir información cifrada cuando se trata de información confidencial. Debe permitir transmitir utilizando un canal de transporte seguro (SSL: Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web) u otro mecanismo estándar.
RNF-SEGFI.09	Debe soportar los estándares LDAP v3 (Protocolo Ligero de Acceso a Directorio), Microsoft ADS (Microsoft Advertising).
RNF-SEGFI.10	El producto deberá brindar mecanismos para cifrar los datos en transporte, almacenamiento y respaldo (encriptación, enmascaramiento).
RNF-SEGFI.11	Debe tener capacidad para dar soporte de seguridad a nivel de servicios (web services) con protocolos estándares.
RNF-SEGFI.12	El producto debe utilizar mecanismos para prevenir vulnerabilidades de seguridad. En particular debe adherirse a estándares de seguridad de industria para aplicaciones Web, tales como OWASP Top-10 (documento de los diez riesgos de seguridad más importantes en aplicaciones web según la Fundación OWASP) y CWE/SANS Top 25 (lista de 25 errores de software más peligrosos). Para las pruebas de aceptación se deben hacer pruebas de seguridad que certifiquen que la aplicación Web pasa las pruebas críticas OWASP.
RNF-SEGFI.13	Debe permitir usar (si lo requiere el MdH como alternativa a los mecanismos de autenticación con certificados digitales) mecanismos de autenticación usando passwords "fuertes", con reglas parametrizables de longitud mínima, frecuencia de cambios, tipos de caracteres obligatorios, repeticiones, etc. (en general, buenas prácticas de passwords seguros).
RNF-SEGFI.14	La firma adjudicataria debe firmar un acuerdo de confidencialidad que será suministrado antes de firmar el contrato.
RNF-SEGFI.15	Las obligaciones que adquiere el adjudicatario en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas. En particular los niveles de seguridad de la información a la que tenga acceso la firma consultora, y de los servicios que de este último dependan. Así entonces, el cumplimiento de los requerimientos de seguridad de la información aplica tanto para la firma adjudicataria, así como para cualquier subcontratación que realice, sea de otra firma o persona. La parte subcontratada deberá atender los requerimientos de seguridad.

RNF-SEGFI	Requerimientos de seguridad
RNF-SEGFI.16	Firma Digital Al utilizar firmas y certificados digitales, se deberá cumplir con la legislación vigente (Ley N° 8454 Ley De Certificados, Firmas Digitales Y Documentos Electrónicos y el Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos) por lo tanto los certificados a utilizar son los emitidos por la Autoridad Certificadora creada con la Ley mencionada, que es la Autoridad Certificado del SINPE. Además, se deben utilizar los formatos avanzados de Firma Digital, tal como lo dice la política emitida por la Dirección de Certificados y Firmas digitales del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica (MICITT).
RNF-SEGFI.17	Normativa sobre la Seguridad de la Información que debe cumplir la firma contratada. La empresa adjudicataria deberá implementar la solución adhiriendo a la normativa siguiente definida por el área de Seguridad del Ministerio de Hacienda: Política General de Seguridad de la Información, Política de gestión de activos, Política de Seguridad Física y Ambiental, Política de Seguridad Ligada al Personal, Política de cumplimiento, Política de control de acceso, Política de adquisición, desarrollo y mantenimiento de software de sistemas de información, Política de gestión de comunicaciones y operaciones, Política de gestión de incidentes, Política de gestión de contratistaes, Política de gestión de riesgos, Estándares de seguridad y protección para los diferentes componentes de la plataforma tecnológica “on-premise” y cloud.
RNF-SEGFI.18	Controles y requerimientos para verificación y gestión de sesiones. La solución ofertada debe garantizar buenas prácticas de seguridad en el manejo de sesiones asegurando, entre otros, que: • Las aplicaciones nunca revelen tokens de sesión en los parámetros de URL.

RNF-SEGFI	Requerimientos de seguridad
	• Las aplicaciones generen un nuevo token de sesión en la autenticación de usuario. • Los tokens de sesión proporcionen al menos 64 bits de entropía. • La aplicación solo almacene tokens de sesión en el navegador usando métodos seguros, como cookies debidamente protegidas (con sus flags). • El token de sesión se genere utilizando criptografía adecuada y reconocida ampliamente. • El cierre de sesión y el tiempo de la caducidad invaliden el token de sesión, de modo tal que el botón de retroceso o una parte de confianza posterior no reanude una sesión autenticada, incluso a través de las partes de confianza.
RNF-SEGFI.19	Controles y requerimientos para validación, higienización y codificación La solución ofertada debe garantizar buenas prácticas de seguridad en validación, higienización y codificación asegurando, entre otros, que: • La aplicación tenga defensas contra ataques HTTP (protocolo de transferencia de hipertextos), particularmente si el marco de la aplicación no hace distinciones sobre el origen de los parámetros de solicitud (GET (el método GET envía los datos usando la URL), POST (el método POST envía los datos de forma que no podemos verlos), cookies, encabezados o variables de entorno). • Los frameworks se protejan contra ataques de asignación de parámetros masivos, o que la aplicación tenga contramedidas para proteger contra asignaciones de parámetros inseguras, como marcar campos como privados o similares. • Todas las entradas (campos de formulario HTML, solicitudes REST, parámetros de URL, encabezados HTTP, cookies, archivos por lotes, fuentes RSS (formato de estructuración de datos en XML que facilita el acceso automatizado a la información contenida en un sitio de Internet), etcétera estén validadas mediante validación positiva (listas de permisos).

RNF-SEGFI	Requerimientos de seguridad
	• Los redireccionamientos y reenvíos de URL (Localizador de Recursos Uniforme por su sigla en inglés) solo permitan destinos que estén en una lista de permitidos, o que muestren una advertencia al redireccionar a contenido potencialmente no confiable. • La aplicación este protegida contra ataques SSRF, mediante la validación de datos no confiables o metadatos de archivos HTTP, como nombres de archivos y campos de entrada de URL; y que utilice listas de permisos de protocolos, dominios, rutas y puertos. • Los datos no estructurados sean higienizados cumpliendo medidas genéricas de seguridad tales como caracteres permitidos, longitud y que caracteres potencialmente dañinos en cierto contexto sean anulados (p. Ej. Nombres naturales con unicode o apóstrofos).
RNF-SEGFI.20	**Controles y requerimientos para verificación de registros y manejo de errores** La solución ofertada debe garantizar buenas prácticas de seguridad en verificación de registros y manejo de errores asegurando, entre otros, que: • La aplicación no registre credenciales o detalles de pago. Los tokens de sesión solo deben almacenarse en registros en forma de hash irreversible. • La aplicación no registre datos confidenciales innecesarios como se define en las leyes de protección de datos de Costa Rica o la política de seguridad relevante. • Los controles del registro de seguridad proporcionen la capacidad para registrar las autenticaciones exitosas y sobre todo los eventos de falla que son identificados como relevantes para la seguridad. • Cada registro de evento incluya la información necesaria para permitir una eventual investigación y correlación con otros eventos. • Los registros de seguridad estén protegidos contra accesos y modificaciones no autorizados. El manejo de excepciones (o un equivalente funcional) se use en todo el código del sistema para tener en cuenta las

RNF-SEGFI	Requerimientos de seguridad
	condiciones de error esperadas e inesperadas de tal forma que se muestre un mensaje genérico cuando se produzca un error inesperado o sensible a la seguridad o con una identificación única, para que el personal de soporte pueda usar e investigar.
RNF-SEGFI.21	**Controles y requerimientos para protección de datos** La solución ofertada debe garantizar buenas prácticas de seguridad en protección de datos asegurando, entre otros, que: • Las aplicaciones protejan los datos confidenciales para que no se almacenen en el cache del servidor, como balanceadores de carga y caches de aplicaciones. • Todas las copias que estén almacenadas en cache o de manera temporal, estén protegidos del acceso no autorizado / invalidar después de que el usuario autorizado acceda a los datos confidenciales. • Las aplicaciones minimicen la cantidad de parámetros en una solicitud, como campos ocultos, variables ajax, cookies y valores de encabezados [(headers.value ()]. • Las aplicaciones puedan detectar y alertar sobre números anormales de solicitudes, como por ip, usuario, total por hora o día, o lo que tenga sentido para la aplicación. • La aplicación establezca suficientes encabezados anti-cache para que los datos confidenciales no se almacenen en el cache de los nuevos navegadores. • Los datos autenticados se borren del almacenamiento del cliente, como el DOM (Document Object Model) del navegador, después de que finalice el cliente o la sesión. • La información confidencial o privada que se requiere cifrar esté cifrada mediante algoritmos aprobados que brinden tanto confidencialidad como integridad.
RNF-SEGFI.22	**Controles y requerimientos para verificación de código malicioso** La solución ofertada debe garantizar buenas prácticas de seguridad en la verificación de código malicioso asegurando, entre otros, que: • El código fuente de los desarrollos o ajustes a la aplicación, y

RNF-SEGFI	Requerimientos de seguridad
	las bibliotecas de terceros no contengan funciones no autorizadas de recopilación de datos. Cuando exista dicha funcionalidad, se debe obtener el permiso del usuario para que funcione antes de recopilar cualquier dato. • La aplicación no solicite permisos innecesarios o excesivos para funciones relacionadas con la privacidad, como contactos, cámaras, micrófonos o ubicación. • La aplicación tenga una función de actualización automática de cliente o servidor, y deban obtenerse a través de canales seguros y firmadas digitalmente. El código de actualización debe validar la firma digital de la actualización antes de instalar o ejecutar la actualización. • La aplicación emplee protecciones de integridad, como la firma de código. La aplicación no debe cargar ni ejecutar código de fuentes no confiables, como la carga de inclusiones, módulos, complementos, código o bibliotecas de fuentes no confiables o de internet.
RNF-SEGFI.23	**Controles y requerimientos para servicios web y API** La solución ofertada debe garantizar buenas prácticas de seguridad para servicios Web y APIs.
RNF-SEGFI.24	**Controles y requerimientos para control de acceso** La solución ofertada debe garantizar buenas prácticas de seguridad en el control de acceso asegurando, entre otros, que: • Todos los atributos de usuario y datos e información utilizados por la política de control de acceso no puedan ser manipulados por los usuarios finales sin la autorización específica. • Los datos confidenciales y las APIs estén protegidos contra ataques de referencia directa de objetos inseguros (IDOR) dirigidos a la creación, lectura, actualización y eliminación de registros, como crear o actualizar el registro de otra persona, ver los registros de todos o eliminar todos los registros.
RNF-SEGFI.25	**Análisis de vulnerabilidades, pruebas de penetración y Auditoría** La firma consultora de la solución debe realizar análisis de vulnerabilidades y de penetración en la medida que van saliendo en vivo partes del sistema, entregar los resultados al MdH y resolver todos los hallazgos para la entrega final del producto.

RNF-SEGFI	Requerimientos de seguridad
RNF-SEGFI.26	La firma consultora deberá implementar los mecanismos de autenticación a los sistemas que desarrolle para el MdH por medio de mecanismos de certificados-firmas digitales provistos por el MdH. La solución deberá interactuar con este mecanismo, cuando estos estén disponibles. Mientras no se encuentren disponibles, debe implementar un mecanismo alterno de autenticación basado en un esquema de Single Sign On, y debería ser a través de alguno de los siguientes protocolos: SAML 2.0 (estándar de código abierto basado en XML que permite el intercambio de información), Oauth 2.0 (estándar abierto para la autorización de APIs), OpenID Connect 1.0 (protocolo de identidad simple y de estándar abierto basado en el protocolo OAuth 2.0).
RNF-SEGFI.27	La firma consultora deberá integrar la autenticación de usuarios de los sistemas que desarrolle para el MdH con el gestor de identidades definido por el Ministerio de Hacienda, preservando las credenciales del usuario de manera tal que no sea requerida nuevas autenticaciones.

7.18 Monitoreo

RNF-MON	Requerimientos de Monitoreo
RNF-MON.01	El sistema debe permitir que mediante un componente (propio) protocolo específico como HTTP o SNMP (protocolo simple administración de redes) pueda ser invocado desde la herramienta monitoreo central del MdH, facilitando la captura de las métricas utilización del sistema, tiempos de respuesta, latencia de la aplicació y estado de salud general de la solución.
RNF-MON.02	El sistema debe proveer mecanismos de detección de fallas, y que con mínimo: • Detecten, registren y notifiquen las excepciones del sistema. • Generen mensajes específicos para cada tipo de excepción, que sean descriptivos y contengan información que ayude a detectar errores, sin exponer información sensible.

7.19 Confiabilidad, integridad y recuperación

RNF-INTEG-8	Requerimientos de confiabilidad, integridad y recuperación
RNF-INTEG-.01	Todas las transacciones con actualizaciones deben ser atómicas y deben permitir recuperar el estado de los datos al comienzo de la ejecución de la transacción en el evento de que ocurran fallas antes de finalizar (hacer un commit/rollback).
RNF-INTEG-.02	La solución debe incluir mecanismos de alerta temprana sobre posibles fallas generadas en componentes de la aplicación o software base, como por ejemplo llenado de logs de auditoría, procesos en cola por tiempos no normales, “timeouts”, conexiones abiertas no previstas.
RNF-INTEG-.03	Debe poder gestionar las excepciones del sistema retornando al menos un código, nombre, origen y causa de la excepción.
RNF-INTEG-.04	La solución ofertada debe garantizar un RTO (Recovery Time Objective) de 2 horas y un RPO (Recovery Point Objective) de 15 minutos.
RNF-INTEG-.05	La solución completa debe estar en capacidad de recibir y procesar mensajes en un proceso de recuperación de fallas.
RNF-INTEG-.06	La firma consultora deberá definir, documentar y poner en operación los procedimientos de respaldos que garanticen la protección de los datos cumpliendo con los acuerdos de nivel de servicio definidos.
RNF-INTEG-.07	La firma consultora debe garantizar que los sistemas desarrollados para el Ministerio de Hacienda soporten la recuperación a partir de los respaldos, garantizando la consistencia de datos y de las operaciones.
RNF-INTEG-.08	La firma consultora debe implementar una estrategia de recuperación de desastres sobre el sistema que permita el cumplimiento de los acuerdos de nivel de servicio definidos.

7.20 Escalabilidad

RNF-ESC	Requerimientos de escalabilidad
RNF-ESC.01	La solución operada en la nube debe permitir escalar horizontal o verticalmente la infraestructura en forma automática y de manera elástica, soportando la demanda habitual y los posibles picos de demanda en momentos inesperados, sin interrupción del servicio y sin necesidad de hacer cambios en la aplicación.
RNF-ESC.02	La solución debe escalar de tal forma que, si se incrementa el número de usuarios en cualquier porcentaje, el costo de los recursos de memoria y computación y comunicaciones en la nube no crecen en un porcentaje mayor al porcentaje de incremento.

7.21 Interoperabilidad

RNF-INTOP	Requerimientos de interoperabilidad
RNF-INTOP.01	El proveedor debe implementar las interfaces necesarias para cumplir con lo especificado en el apartado ***5. Modelo Conceptual de SUPRES*** en lo referente a recepción y envío de información a los sistemas con los cuales se relaciona. Para ello se provee en el Anexo XXX el listado de las interfaces identificadas.
RNF-INTOP.02	La implementación de la interoperabilidad de SUPRES debe facilitar la comunicación confiable entre recursos de TI tal como aplicaciones, plataformas y servicios que están distribuidos en múltiples sistemas internos y externos al MdH, en múltiples nubes, utilizando mecanismos de integración requeridos tales como: • Servicios Web basados en protocolo SOAP sobre protocolos diversos tales como HTTP/HTTPS, SMTP, TCP, UDP. • API REST sobre protocolos HTTP/HTTPS, FTP/FTPS, SFTP soportando diversos formatos de mensaje, tales como HTML, XML, JSON, entre otros. • Intercambio de archivos en diversos formatos tales como TXT, CSV, entre otros. • Conectores con Base de Datos estructuradas tales como DB2, Microsoft SQL, MySQL y Oracle, entre otras (p. Ej., ODBC, JDBC, ADO) y no estructuradas, sea que se ubiquen en nube pública, nube privada o nube híbrida, o instalaciones “On Premises”. • Mensajería (MQ). • TCP/IP Sockets. Lo anterior de acuerdo con las necesidades y posibilidades de los sistemas externos al SUPRES.
RNF-INTOP.03	El producto debe brindar soporte a la implementación de las capacidades descritas en la capa de Integración de la Arquitectura de Referencia SOA del OpenGroup (http://www.opengroup.org/soa/source-book/soa_refarch/p13.htm)
RNF-INTOP.04	Los mensajes electrónicos de intercambio de información entre este sistema y los diferentes sistemas deberán contar con la especificación WADL/WSDL.
RNF-INTOP.05	El proveedor debe implementar los intercambios de información requeridos por el SUPRES de manera independiente con respecto a la tecnología existente en los sistemas externos, sean fuente o destino, de los intercambios, de tal manera que dichos sistemas externos puedan ser sustituidos sin que esto represente una modificación en SUPRES.

RNF-INTOP	Requerimientos de interoperabilidad
RNF-INTOP.06	La solución a desarrollar debe ser compatible con: • Simple Object Access Protocol (SOAP) • SOAP Message Transmission Optimization Mechanism (MTOM) • XML-Binary Optimized Packaging (XOP) • WS-I Basic Profile • Universal Description Discovery and Integration (UDDI) Client • WS-Atomic Transaction • WS-I Basic Security Profile- • WS-Security Specification
RNF-INTOP.07	Debe soportar todos los protocolos estándar de definición de servicios Web definidos en el WS-I Basic Profile en sus últimas versiones.
RNF-INTOP.08	El sistema debe permitir la integración con un componente de monitoreo y salud de componentes de aplicaciones.
RNF-INTOP.09	El sistema debe poder integrarse con un administrador de Políticas de Servicio para el trabajo con protocolos de servicios más avanzados, como por ejemplo WS-Trust, WS-Security, WS-Addressing y WS-I Basic Security Profile.
RNF-INTOP.10	El sistema debe permitir modalidades de comunicación síncronas y asíncronas.
RNF-INTOP.11	La solución debe tener la capacidad de adicionar, modificar o eliminar servicios sin afectar la operativa del resto de los servicios configurados.
RNF-INTOP.12	La solución debe tener la capacidad de aplicar políticas de seguridad independientes por servicio.
RNF-INTOP.13	La solución debe permitir desarrollar interfaces particulares para la integración con sistemas o interfaces legadas.
RNF-INTOP.14	La solución debe brindar posibilidad de configurar mecanismos de reintentos para la llamada a servicios.
RNF-INTOP.15	Deberá brindar soporte para la validación de firmas y gestión de certificados para la autenticación de servicios.
RNF-INTOP.16	La solución deberá garantizar la auditoría de todos los cambios en los servicios.
RNF-INTOP.17	Debe brindar mecanismos para exponer múltiples versiones de un mismo servicio.
RNF-INTOP.18	La solución deberá permitir gestionar los flujos no exitosos para resolverlos y reactivarlos.
RNF-INTOP.19	El valor de la solución no debe estar relacionado con la cantidad de mensajes o tráfico que genera su interoperabilidad con otros sistemas.

RNF-INTOP	Requerimientos de interoperabilidad
RNF-INTOP.20	Los servicios web desarrollados como producto de este contrato deberán portables a otras plataformas de interoperabilidad, indistintamente sean estas en “on premises” o nube, para lo cual el MdH indicará dicha plataforma destino.
RNF-INTOP.21	La firma consultora debe incluir todas las actividades técnicas necesarias para realizar las integraciones de los sistemas desarrollados para el Ministerio de Hacienda con sistemas y plataformas internas o externas al MdH.
RNF-INTOP.22	La firma consultora debe modelar en detalle las integraciones y los flujos de información entre la solución y los sistemas de información internos y externos utilizando herramientas apropiadas para ello. Por ejemplo, el flujo de una transacción que se comunica una o varias veces con un sistema externo o con varios sistemas, qué hace, qué pasa si hay errores, si hay timeouts, etc.
RNF-INTOP.23	La firma consultora debe definir un diccionario de datos que defina la semántica y sintaxis de los datos que requiere intercambiar, y debe garantizar que se estandarice con el de los otros sistemas Core, incluyendo entre otros elementos: datos, descripción, estructura de los datos (tipo de dato, longitud, etc.), reglas de negocio y validaciones, contratista de la información, consumidores de la información, gestión de seguridad, gestión de errores.
RNF-INTOP.24	La firma consultora debe implementar las interfaces de la solución con los sistemas de información internos y externos al MdH, usando el bus de integración implementado por el MdH.
RNF-INTOP.25	La firma consultora debe elaborar la documentación técnica y funcional de cada interfaz de la solución con otros sistemas de información, que incluya, como mínimo, el diseño final, los puntos de integración, diccionario de datos semántico y sintáctico, aspectos técnicos de seguridad, flujos de información, conexiones y mensajes de error.

7.22 Operación en la nube

RNF-NUB	Requerimientos de nube
RNF-NUB.01	La solución debe funcionar de manera óptima en cualquiera de las nubes que aparecen en el cuadrante de Líderes en servicios de infraestructura y plataforma, según el último estudio de Gartner.

RNF-NUB.02	La firma consultora deberá dar soporte y mantenimiento de la solución instalada en cualquiera de las nubes que aparecen en el cuadrante de Líderes en servicios de infraestructura y plataforma, según el último estudio de Gartner, en modalidad IaaS o máquinas virtuales.
RNF-NUB.03	El oferente debe entregar al MdH la configuración detallada de arquitectura de nube requerida por la solución ofertada. Incluye la lista de todos los servicios de nube con sus respectivos dimensionamientos, capacidades y relacionamientos para las necesidades del MdH. Debe especificar el plan progresivo de uso de los recursos, la arquitectura tecnológica, esquema de comunicaciones y redes, entre otros elementos según lo indicado en el Diseño de Infraestructura.
RNF-NUB.04	La firma consultora (en la eventualidad de que el Ministerio de Hacienda no haya aprovisionado el servicio de nube a partir de la finalización de la Fase de Implementación) deberá iniciar la misma en una instancia de nube provista por él, debiendo realizar la migración a la nube definida por el Ministerio de Hacienda en el momento que se le indique. Se estima que el plazo máximo para esta definición será de 6 meses, una vez inicie el contrato. Nota: Si al iniciar con la parametrización de la solución el Ministerio de Hacienda ha aprovisionado el servicio de nube, lo indicado no será requerido y el MH no pagará por este rubro. En caso se utilice el servicio por un plazo menor a 6 meses se pagará por el tiempo utilizado. Al cabo de dicho plazo, los sistemas desarrollados, con todos sus ambientes deberán ser trasladados a la nube que indique el Ministerio de Hacienda.
RNF-NUB.05	La firma consultora será responsable del correcto funcionamiento y operación de la solución en la nube en sus diferentes ambientes, debiendo cumplir los requerimientos relacionados con el desempeño y rendimiento de la solución en el ambiente de Producción definidos en este documento.
RNF-NUB.06	Todas las cuentas de los servicios y derechos de uso sobre la totalidad de los componentes de software de la solución implementada en la Nube deberán estar a nombre del MdH.
RNF-NUB.07	El oferente deberá transferir el conocimiento de la operación de la nube en sus diferentes ambientes a los funcionarios que el MdH designe para tal efecto.
RNF-NUB.08	El sistema debe ser integrado con el gestor de identidades del Ministerio de Hacienda (MdH) para la administración de los usuarios que ingresan al sistema.

7.23 Rendimiento de la solución

La solución DEBERÁ alcanzar los siguientes niveles de rendimiento:

<table>
<tr><th>RNF-REND</th><th>Requerimientos de rendimiento del sistema informático</th></tr>
<tr><td>RNF-REND.01</td><td>El software desarrollado para ser operado en la nube debe estar implementado con tecnologías que permitan el despliegue de la solución bajo esquemas de alta disponibilidad y balanceo de carga.</td></tr>
<tr><td>RNF-REND.02</td><td>La solución implementada en sus diferentes ambientes debe estar en capacidad de operar en los siguientes esquemas de disponibilidad.

<table><tr><td>Desarrollo</td><td>98%</td></tr><tr><td>Calidad</td><td>98%</td></tr><tr><td>Homologación</td><td>98%</td></tr><tr><td>Producción</td><td>99,9%</td></tr></table></td></tr>
<tr><td>RNF-REND.03</td><td>La solución ofertada con el dimensionamiento de Nube debe soportar la cantidad de mensajes intercambiados considerando períodos y/o días pico (el número aproximado de 400.000 transacciones entre 5 días). El tiempo máximo para una transacción en línea para lo que corresponde al aplicativo no debe superar un tiempo promedio de 3 segundos.</td></tr>
<tr><td>RNF-REND.04</td><td>En general, el tiempo máximo para una transacción en línea para lo que corresponde al aplicativo no debe superar un tiempo promedio de 3 segundos.</td></tr>
<tr><td>RNF-REND.05</td><td>En caso de que la firma consultora incumpla con niveles de servicio referentes a tiempo promedio de respuesta de la aplicación o el nivel de disponibilidad (3 segundos), el Contratante le impondrá una multa cuyo importe corresponderá a un 0,25% sobre el monto correspondiente al alquiler de la nube.</td></tr>
<tr><td>RNF-REND.06</td><td>En cuanto al procesamiento de los mensajes relacionados con el ingreso de solicitudes de pago, se trata de una aplicación crítica. Por lo tanto, requiere de una disponibilidad de las 24 horas, los 365 días del año.

Con el fin de asegurar el cumplimiento de lo anterior, la siguiente tabla define los tiempos máximos para el procesamiento de los mensajes en la solución desarrollada:

<table><tr><th>Descripción</th><th>Tiempo máximo para brindar la respuesta</th></tr><tr><td>En la recepción y validación de mensajes que requieran respuesta al remitente, contando el tiempo a partir del momento en que es recibido el mensaje y hasta que se responde al remitente con el resultado de la validación,</td><td>250 milisegundos</td></tr></table></td></tr>
</table>

<table>
<tr><td>RNF-REND</td><td>Requerimientos de rendimiento del sistema informático</td></tr>
<tr><td></td><td>
<table>
<tr><td>debiendo descontarse los tiempos de espera de sistemas externos a la solución implementada.</td><td></td></tr>
</table>
Cuando se incumpla con el nivel de servicio de rendimiento de la aplicación descrito, se catalogará en el impacto de la siguiente manera:
<table>
<tr><td></td><td></td><td colspan="3">Catalogación del impacto</td></tr>
<tr><td>Grado</td><td>Condición de incumplimiento</td><td>Durante un lapso entre 15 y 30 minutos</td><td>Durante un lapso entre 31 y 60 minutos</td><td>Durante un lapso superior a 1 hora</td></tr>
<tr><td>1</td><td>El tiempo promedio de respuesta es superior a 250 milisegundos y menor o igual a 375 milisegundos</td><td>Bajo</td><td>Medio</td><td>Alto</td></tr>
<tr><td>2</td><td>El tiempo promedio de respuesta es superior a 375 milisegundos y menor a 500 milisegundos</td><td>Medio</td><td>Medio</td><td>Alto</td></tr>
<tr><td>3</td><td>El tiempo promedio de respuesta es superior a 500 milisegundos</td><td>Medio</td><td>Alto</td><td>Alto</td></tr>
</table>
La acumulación del tiempo de incumplimiento se hará en incrementos de minutos cumplidos. Para efectuar el cálculo de la multa el mismo sistema sumará todos los tiempos acumulados de incumplimiento durante el mes de servicio.
</td></tr>
</table>

<table>
<tr><th>RNF-REND</th><th>Requerimientos de rendimiento del sistema informático</th></tr>
<tr><td>RNF-REND.07</td><td>Para el control del rendimiento de la aplicación y verificar el cumplimiento de estos niveles de servicio, la firma consultora debe habilitar un sistema de monitoreo que almacene los datos de tiempos de respuesta acumulados del servicio, el cual debe ser accesible para que el equipo técnico del Ministerio pueda obtener información del comportamiento del servicio. Este monitoreo deberá alertar vía correo electrónico cuando uno de estos acuerdos se esté incumpliendo. La información almacenada deberá permitir generar reportes de incumplimiento de los niveles de servicio, según su impacto y con acumulación del tiempo de incumplimiento, para rangos de fechas configurables.</td></tr>
<tr><td>RNF-REND.08</td><td>En el caso de que para un período de servicio ocurra un incumplimiento de los niveles de servicio para el procesamiento de mensajes, se aplicará una multa, de acuerdo con lo siguiente, salvo casos de fuerza mayor debidamente justificados:

Para el cálculo de la multa se utilizará la siguiente fórmula:

(% de multa de incumplimiento) * (tiempo acumulado de incumplimiento de niveles de servicios) * (monto de servicio de nube del mes anterior)

Dónde:
% de multa de incumplimiento: Es el valor porcentual asociado al impacto del evento, según se establece a continuación:
<table>
<tr><th>Impacto</th><th>% de multa de incumplimiento</th></tr>
<tr><td>Alto</td><td>2,5%</td></tr>
<tr><td>Medio</td><td>1,5%</td></tr>
<tr><td>Bajo</td><td>0,5%</td></tr>
</table>

<u>Tiempo acumulado de incumplimiento de nivel de servicio:</u> Es el acumulado del tiempo de los eventos de incumplimiento del nivel de servicio durante el mes, que están asociados a un determinado impacto.</td></tr>
</table>

RNF-REND	Requerimientos de rendimiento del sistema informático
	Monto de servicio de nube del mes anterior: Corresponde al valor de la factura por el servicio de nube ofrecido por la firma consultora al Ministerio de Hacienda para la operación de la solución implementada.

7.24 Actualización de la solución

RNF-ACT	Requerimientos de actualización de la solución
RNF-ACT.01 .	La solución debe brindar mecanismos que permitan el despliegue e instalación de las actualizaciones sin interrupción de los servicios prestados por la plataforma y en forma continua y en lo posible automatizada desde el entorno de desarrollo hasta producción (“DevOps”).

8. Requerimientos de personal

PER	Requerimientos de actualización de la solución
PER.01	El Consultor deberá proveer el siguiente Personal Profesional: a) Cargo P-1: Administrador de Proyectos b) Cargo P-2: Líder Responsable. c) Cargo P-3: Encargado de Calidad e) Cargo P-4: Encargado de Seguridad f) Equipo de Desarrollo
PER.02	El Administrador de Proyectos debe cumplir con los siguientes requisitos: • Grado universitario mínimo de bachiller en una carrera afín al desarrollo de software • Contar con certificación PMP o equivalente o contar con una maestría en administración de proyectos • Haber aprobado cursos de metodologías ágiles, o contar con una certificación en metodologías ágiles • Experiencia de al menos 4 años ejerciendo el rol de director de proyectos de desarrollo de sistemas de información • Capacidad de comunicación oral y escrita en idioma español
PER.03	El Administrador de Proyectos designado por la firma consultora deberá cumplir con las siguientes responsabilidades:

	- Realizar la gestión general del proyecto por parte de la firma consultora. - Llevar el control del cumplimiento del plan de proyecto general y su cronograma. - Preparar los informes y presentaciones de diferentes aspectos del proyecto. - Asistir a las reuniones donde se requiera informar del estado del proyecto. - Coordinar con las contrapartes designadas por el MdH para el desarrollo de las actividades del proyecto. - Velar porque el proyecto marche de forma adecuada, alertando de posibles desviaciones, riesgos o cambios que puedan afectar el cumplimiento de los objetivos.
PER.04	El Líder Responsable debe cumplir con los siguientes requisitos: • Grado universitario mínimo de bachiller en una carrera afín a desarrollo de software. • Contar con la certificación en metodología ágil que lo acredite como capacitado para ejercer este rol, que haya sido otorgada por una entidad especializada en brindar capacitación de metodologías ágiles. • Experiencia de 4 años estando a cargo de la aplicación de la metodología ágil propuesta en proyectos de desarrollo de software. • Capacidad de comunicación oral y escrita en idioma español.
PER.05	El Líder Responsable designado por la firma consultora deberá cumplir con las siguientes responsabilidades: • Velar porque el Equipo de Desarrollo, el representante del negocio designado por el Ministerio de Hacienda, y resto de participantes cumplan de manera correcta con el rol asignado dentro del proyecto, de acuerdo con la metodología ágil propuesta. • Velar porque las ceremonias y procesos de la metodología ágil propuesta sea llevadas de manera correcta. • Velar porque el Equipo de Desarrollo cuente con las herramientas necesarias para realizar el trabajo. • Participar en la identificación de los interesados del proyecto. • Velar porque los recursos de respaldo estén disponibles. • Apoyar al representante del negocio en la creación de los insumos que debe aportar según la metodología ágil propuesta. • Apoyar al Equipo de Desarrollo en las actividades requeridas para la planificación de cada ciclo corto de desarrollo.

	• Coordinar las actividades para planificación del lanzamiento de producto. • Facilita las reuniones del Equipo de Desarrollo para garantizar que se cumplen los objetivos. • Apoyar al Equipo de Desarrollo en la creación de los entregables acordados en cada ciclo corto de desarrollo. • Ayudar a actualizar las diferentes herramientas metodológicas utilizadas para apoyar el proceso ágil. • Llevar un registro de tareas completadas. • Llevar un registro de tareas por realizar, por día. • Llevar un registro de los impedimentos u obstáculos que se enfrentan. • Facilitar la presentación de los entregables completados por el Equipo de Desarrollo para la aprobación del representante del negocio.
PER.06	El Encargado de Calidad debe cumplir con los siguientes requisitos: • Grado universitario mínimo de bachiller en una carrera afín a la ingeniería o tecnologías de la información. • Haber aprobado cursos en aseguramiento de calidad en software, o contar con una certificación en calidad de software. • Haber aprobado cursos de metodologías ágiles, o contar con una certificación en metodologías ágiles. • Experiencia de al menos 2 años ejerciendo el rol de encargado de calidad en proyectos de desarrollo de software. • Capacidad de comunicación oral y escrita en idioma español.
PER.07	El Encargado de Calidad debe cumplir lo siguiente: 1. Diseñar el plan de pruebas de la pila priorizada, diseñando los casos de prueba que serán aplicados a los entregables desarrollados, 2. Diseñar las tareas requeridas para ejecutar las pruebas de cada entregable desarrollado. 3. Certificar que el código desarrollado es de calidad (siguiendo el procedimiento que brinde arquitectura), 4. Desarrollar los manuales del sistema a colocar en producción.
PER.08	El Encargado de Seguridad debe cumplir con los siguientes requisitos: • Grado universitario mínimo de bachiller en una carrera afín a la ingeniería o tecnologías de la información.

	• Haber aprobado cursos en seguridad de la información, o contar con una certificación en seguridad de la información emitida por una entidad reconocida. • Haber aprobado cursos de metodologías ágiles, o contar con una certificación en metodologías ágiles. • Experiencia de al menos 2 años ejerciendo el rol de encargado de seguridad en proyectos de desarrollo de software. • Capacidad de comunicación oral y escrita en idioma español.
PER.09	El Encargado de Seguridad debe cumplir lo siguiente: 1. Concientizar al Equipo de Desarrollo en seguridad de la información y los requerimientos definidos por el MdH para la solución a desarrollar. 2. Asesorar al Equipo de Desarrollo para que consideren aspectos de seguridad durante las fases de análisis, diseño y desarrollo de los entregables y las pruebas. 3. Realizar el modelado de amenazas en cada ciclo corto de desarrollo y en el lanzamiento del producto 4. Apoyar al Equipo de Desarrollo identificando amenazas, vulnerabilidades y proponiendo medidas de remediación (controles). 5. Identificar herramientas y marcos de trabajo para realizar análisis relacionados con la seguridad. 6. Participar en la redacción y ejecución de los escenarios de casos de prueba relacionados con seguridad de la información. 7. Emitir criterio sobre el cumplimiento de los requerimientos de seguridad por parte de la solución implementada.
PER.10	Los integrantes del Equipo de Desarrollo deben cumplir los siguientes requisitos: a. Contar con grado universitario en Ingeniería Informática o carrera afín b. Contar con una experiencia mínima de 2 años en proyectos de desarrollo y mantenimiento de sistemas de información, utilizando metodologías ágiles. c. Contar con una experiencia mínima de 2 años en desarrollo de software utilizando lenguajes orientados a objetos. d. Deben contar con una experiencia mínima de 2 años en proyectos de desarrollo y/o mantenimiento de APIs. e. Debe incluir un encargado de calidad (QA), un encargado de experiencia de usuario (UX/UI) y un experto en seguridad de nube (SA). f. Capacidad de comunicación oral y escrita en español.

PER.11	Corresponderá al Equipo de Desarrollo cumplir con las siguientes responsabilidades: • Entender y estimar las tareas de desarrollo a realizar en los ciclos cortos de desarrollo. • Funcionar de manera auto-organizada • Debe cumplir con los entregables comprometidos en cada uno de los ciclos cortos de desarrollo. • Busca clarificación sobre nuevos productos o cambios en los productos existentes. • Desarrollar una lista de tareas detallada a cumplir para cumplir con los entregables acordados. • Crea Entregables. • Identificar riesgos e implementar acciones de mitigación de riesgos. • Actualizar los instrumentos para reportar avances. • Participar en las sesiones de revisión del producto desarrollado. • Identificar las oportunidades de mejora en el proceso de desarrollo.

9. Requerimientos de Aceptación operacional

AO	Descripción
AO.01	La aceptación operacional de la solución implementada requerirá que la firma consultora entregue lo siguiente: • Requerimientos de la solución cumplidos satisfactoriamente. • Etapa de Estabilización cumplida de manera satisfactoria. • Solución implementada, incluyendo el código fuente, debidamente documentado. • Documentación generada durante el proyecto. • Capacitación y transferencia de conocimiento realizada al personal de MdH.
AO.02	La puesta en operación de la solución implementada tendrá como prerrequisito haber sido entregado a la mesa de servicio del MdH, cumpliendo con los procedimientos y protocolos definidos para estos efectos, incluyendo capacitación a los agentes de servicio de nivel 1 y la definición de los niveles de escalamiento a los niveles superiores.

AO	Descripción
AO.03	La firma consultora debe brindar acompañamiento al Ministerio de Hacienda durante la puesta en operación de los diferentes módulos de la plataforma, de forma tal que el proceso resulte expedito.

10. Requerimientos de Garantía

La solución desarrollada debe contar con una garantía técnica por parte de la firma consultora, la cual deberá cubrir cada módulo o componente de la solución ante cualquier mal funcionamiento o error producido en el proceso de desarrollo en la implementación de la solución. El período de la garantía será de 12 meses contados a partir de la aceptación operacional de la solución integrada. Las mejoras realizadas como producto del Mantenimiento Evolutivo tendrán también un período de 12 meses de garantía a partir de la puesta en operación de cada mejora. Durante el periodo de garantía la firma consultora debe ofrecer los siguientes servicios:

GAR-	Descripción
GAR.01	Garantizar que se atenderán y resolverán las fallas derivadas del diseño, vulnerabilidades de seguridad de la información, la mano de obra o de cualquier acto de acción u omisión de la firma consultora durante el Contrato cumpliendo con las condiciones definidas en la sección Atención de Incidentes, sin costo adicional para el Ministerio de Hacienda, aun cuando no exista un nuevo contrato con la firma consultora.
GAR.02	Garantizar que las funcionalidades de la solución cumplen 100% de los requerimientos funcionales y no funcionales.
GAR.03	Garantizar que con el uso y entrada de usuarios a la solución el desempeño de la solución se mantiene estable y no se degrada.
GAR.04	Participar en reuniones periódicas para hacer seguimiento a la atención y solución de incidentes y problemas que se presenten en la solución.
GAR.05	Suministrar e instalar las actualizaciones, parches, correcciones y releases para los componentes de la solución sin costo adicional.
GAR.06	Actualizar la documentación del software, reflejando las características y funcionalidades actualizadas de la solución.

GAR-	Descripción
GAR.07	El período de la garantía será de 12 meses contados a partir de la aceptación operacional de la solución integrada.