INFORME DE EVALUACIÓN

En la ciudad de Asunción, capital de la República del Paraguay, a los 22 días del mes de agosto del año 2017, se presenta el Informe Final resultante de la Evaluación de ofertas inherente a la **LICITACIÓN PÚBLICA NACIONAL SBE N° 172/16 "ADQUISICIÓN DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017"**, elaborado en base a lo establecido en el artículo 26 de la Ley N° 2051/2003 de "CONTRATACIONES PÚBLICAS", el Art. 61 del Decreto N° 21.909 que reglamenta la Ley N° 2.051/2003 de "CONTRATACIONES PÚBLICAS" y el Decreto N° 5.174 por el cual se modifican algunos artículos del Decreto N° 21.909/2003, y demás artículos concordantes, a efectos de elevarlo a consideración de la Presidencia del Instituto de Previsión Social y por su intermedio al Consejo de Administración.-

Por sorteo de fecha 07 de agosto de 2017, realizado en la Coordinación – Dirección Operativa de Contrataciones, se designa a la Comisión Evaluadora de Ofertas, la cual se encuentra integrada por los siguientes funcionarios: el **Miguel Darío Centurión Barreto, Lic. Víctor Ramón Corvalan Giret** en representación de la Dirección de Tecnología de la Información y las Comunicaciones, el **Abg. Leticia Pamela Giménez Mendiola**, en representación de la Dirección Jurídica y el **Lic. Herminio Ramón Rivas**, en representación de la Dirección Operativa de Contrataciones.-

1. ANTECEDENTES

Que, por Nota Interna GDG/DTIC/N° 203/16, registrada como NOT-0052-2016-000173 de fecha 3 de noviembre de 2016, la Dirección de Tecnología de la Información y Comunicaciones, remite el pedido de **"ADQUISICIÓN DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS".**

Que, el Departamento Técnico de Contrataciones por Memorándum DOC/DTC/ N° 0018/2017 de fecha 06 de enero de 2017, informo que se procedió a la inclusión en el PAC 2017, el llamado correspondiente a la **"ADQUISICIÓN DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017"** bajo la modalidad de Licitación Pública Nacional con **ID N° 321.424**.-

Por Resolución N° 005-003/17 de fecha 25 de enero de 2017, el Consejo de Administración resolvió: **Art. 1°)** Autorizar el llamado a **LICITACIÓN PÚBLICA NACIONAL SBE N° 172/16 "ADQUISICIÓN DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017"**, conforme a la normativa legal vigente, y a lo expuesto en el exordio de la presente Resolución, **Art. 2°)** Aprobar el Pliego de Bases y Condiciones de la **LICITACIÓN PÚBLICA NACIONAL SBE N° 172/16 "ADQUISICIÓN DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017".-**

Por Nota **G.A.L.D.O.P. N° 0056/2017** de fecha 31 de enero de 2017, la Dirección Operativa de Contrataciones, comunicó el inicio del llamado de referencia con ID N° 321.424 a la Dirección Nacional de Contrataciones Públicas, indicando que el monto estimado de la contratación corresponde a la suma de G. 3.526.816.000 (Guaraníes Tres mil quinientos veintiséis millones ochocientos dieciséis mil).-

Se realizo la Publicación en Prensa Escrita en fecha 07, 08 y 09 de febrero de 2017.-

Miguel Centurión
Instituto de Previsión Social

INSTITUTO DE PREVISION SOCIAL
Lic. Herminio Ramón Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Corvalán Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

2. DISPONIBILIDAD PRESUPUESTARIA

Por Memorándum **DCP/DPR/PR2 N° 000185/2017** de fecha 20 de enero de 2017, la Sección Ejecución y Control Presupuestario del Departamento de Presupuesto de la Dirección de Contabilidad y Presupuesto, informa que el presente pedido afecta al Objeto de Gasto 570 **"Adquisición de Activos Intangibles"** del Programa 1 "Administración General" y del Programa 2 de **"Servicios Sociales de Calidad".** Dicho llamado cuenta con Reserva presupuestaria por un valor de Gs. 1.975.016.960 (Guaraníes Mil novecientos setenta y cinco millones dieciséis mil novecientos sesenta). Se aclara que el presente llamado no cuenta con el Certificado de Disponibilidad Presupuestaria, por lo que la firma de los contratos respectivos estará sujeta a la emisión de dicho Certificado.-

3. ACTA DE SESIÓN PÚBLICA VIRTUAL

Según Acta de Sesión Pública Virtual, SBE ID N° 321.424 de fecha 03 de agosto de 2017, emitido por la Dirección Nacional de Contrataciones Públicas, participo los siguientes proveedores.-

LISTADO DE PROVEEDORES PARTICIPANTES DE LA SUBASTA A LA BAJA ELECTRONICA:

Nro. Garantía	Tipo	ENTIDAD EMISORA	Fecha Emisión	Fecha Inicio de Vigencia	Fecha Fin de Vigencia
Oferente: LOGICALIS PARAGUAY S.A. - RUC: 80022674-7			**Categoría: Sin categorizar**		**Nro. Oferente: 1**
[illegible]	Poliza	Seguros Chaco S.A.	31-07-2017	03-08-2017	01-03-2018
Oferente: ONE S.A. - RUC: 80064041-1			**Categoría: Sin categorizar**		**Nro. Oferente: 2**
[illegible]	Poliza	La Consolidada de Seguros	01-08-2017	03-08-2017	11-03-2018
Oferente: INFOMARTICA TECNOLOGIA & COMUNICACION - RUC: 80034665-3			**Categoría: Sin categorizar**		**Nro. Oferente: 3**
[illegible]	Poliza	Aseguradora del Este	02-08-2017	02-08-2017	08-02-2018
Oferente: CONSORCIO IDENTIDAD DIGITAL - RUC: DNCP-000769			**Categoría: Sin categorizar**		**Nro. Oferente: 4**
[illegible]	Poliza	La Consolidada S.A. De Seguros	01-08-2017	02-08-2017	10-03-2018
Oferente: STARK TECNOLOGIA S.A - RUC: 80036088-5			**Categoría: Sin categorizar**		**Nro. Oferente: 5**
[illegible]	Poliza	ASEGURADORA PARAGUAYA S.A.	02-08-2017	02-08-2017	03-02-2018

MEJORES LANCES DE CADA PROVEEDOR POR ÍTEM

1 - LPN SBE 172-16 ADQUISICION DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017	
Oferente	**Mejor Precio**
ONE S.A. - 80064041-1	2.200.793.526
CONSORCIO IDENTIDAD DIGITAL - DNCP-000769	3.100.000.000
STARK TECNOLOGIA S.A - 80036088-5	3.119.000.000
INFOMARTICA TECNOLOGIA & COMUNICACION - 80034665-3	3.526.815.000
LOGICALIS PARAGUAY S.A. - 80022674-7	4.200.000.000

INSTITUTO DE PREVISION SOCIAL
Lic. Hermilio Ramón Rivas
DIRECCIÓN OPERATIVA DE CONTRATACIONES

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Corvalán Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

Miguel Centurión
Dpto. de Tecnología
Dirección de Informática
Instituto de Previsión Social

ÍTEMS GANADOS POR PROVEEDOR

Proveedor: 80064041-1 - ONE S.A.	
Item	**Precio Ganador**
1 - LPN SBE 172-16 ADQUISICION DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017	2.200.790.526

4. <u>ACTO DE APERTURA DE SOBRES</u>

Según consta en el **Acta N° 042/17** de fecha 04 de agosto de 2.017, siendo las 08:45 hs. se procedió al cierre del plazo establecido para la presentación de los sobres conteniendo los documentos de oferta de la **LICITACIÓN PÚBLICA NACIONAL SBE N° 172/16 "ADQUISICIÓN DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017".-**

Seguidamente, siendo las 09:00 horas se dio apertura al sobre recepcionado:

1. LOGICALIS PARAGUAY S.A – RUC N° 80022674-7: Según Planilla de Precios cotiza por un Monto Total de **Gs.4.200.000.000.- (Guaraníes Cuatro mil doscientos millones),** Monto de la Garantía de Mantenimiento de Oferta: **Gs.159.000.000.- (Guaraníes Ciento cincuenta y nueve millones)** Empresa Aseguradora: SEGUROS CHACO S.A DE SEGUROS Y REASEGUROS N° de Póliza: 2.1508.13385/000 Total de hojas foliadas 126 (Ciento veinte y seis).

2. ONE S.A - RUC N° 80064041-1: Según Planilla de Precios cotiza por un Monto Total de **Gs.2.200.790.526.- (Guaraníes Dos mil doscientos millones setecientos noventa mil quinientos veinte y seis),** Monto de la Garantía de Mantenimiento de Oferta: **Gs.99.000.000.- (Guaraníes Noventa y nueve millones)** Empresa Aseguradora: LA CONSOLIDADA S.A DE SEGUROS N° de Póliza: 007.1508.039759/000.- Total de hojas foliadas 164 (Ciento sesenta y cuatro).

3. STARK TECNOLOGIA S.A. - RUC N° 80036088-5: Según Planilla de Precios cotiza por un Monto Total de **Gs.3.119.000.000.- (Guaraníes Tres mil ciento diez y nueve millones),** Monto de la Garantía de Mantenimiento de Oferta: **Gs.105.000.000.- (Guaraníes Ciento cinco millones)** Empresa Aseguradora: ASEGURADORA PARAGUAYA S.A ASEPASA N° de Póliza: 18.1508.0013212.0000.- Total de hojas foliadas 56 (Cincuenta y seis).

4. ITC S.A. - RUC N° 80034665-3: Según Planilla de Precios cotiza por un Monto Total de **Gs.3.526.816.000.- (Guaraníes Tres mil quinientos veinte y seis millones ochocientos diez y seis mil),** Monto de la Garantía de Mantenimiento de Oferta: **Gs. 106.000.000.- (Guaraníes Ciento seis millones)** Empresa Aseguradora: ASEGURADORA DEL ESTE S.A N° de Póliza: 45.1508.0008482.000.- Total de hojas foliadas 72 (Ciento Setenta y dos).

<u>OBSERVACIÓN:</u> *Se deja expresa constancia que la firma* **ALIAS S.A** *presenta su oferta fuera del plazo establecido (plazo establecido 8:45 hs.) para la recepción de ofertas, por lo cual no se dio apertura a su sobre oferta.*

Observaciones realizadas por la firma STARK TECNOLOGIA S.A.

- El oferente ONE S.A. no presenta facturas por el 50 % del valor de su oferta inicial.

<u>Respuesta de la Comisión Evaluadora</u>:

Esta Comisión evaluadora realizo las verificaciones de las documentaciones presentadas por la firma ONE S.A., las misma se ajusta al Pliego de Bases y Condiciones.

Observaciones realizadas por la firma LOGICALIS PARAGUAY S.A

- La empresa ITC S.A. no presenta facturas por experiencias en trabajos similares.
- La empresa ITC S.A. solo presenta autorización del mayorista.
- La empresa ONE S.A. no presenta Técnicos certificados

<u>Respuesta de la Comisión Evaluadora</u>:

INSTITUTO DE PREVISION SOCIAL
Lic. Hermilio Ramón Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

INSTITUTO DE PREVISIÓN SOCIAL
Lic. Víctor Corvalán Gire
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicación

Miguel Centurión
Jefe de Seguridad
Dirección de Informática
Instituto de Previsión Social

Punto 1: Esta Comisión realizo las verificaciones en la carpeta oferta y no se han visualizados las facturas correspondientes, por la cual se solicito a la empresa ITC S.A. vía nota N° 772/17, las documentaciones correspondientes.
Punto 2: Esta Comisión verifico en la carpeta y se ha observado la autorización del fabricante.
Punto 3: Se ha observado en la carpeta del oferente, la presentación del documento que avala que el técnico de la empresa referida posee certificación.

Observaciones realizadas por la firma ONE S.A

- La empresa ITC S.A. no presenta autorización del Fabricante, presenta solo autorización del mayorista local.
- La empresa ITC S.A. no presenta facturas/contratos que demuestren haber provenidos la solución de gestión de identidades

Respuesta de la Comisión Evaluadora:
Punto 1: Esta Comisión ha observado en la carpeta del oferente la autorización del fabricante.
Punto 2: Esta Comisión realizo las verificaciones en la carpeta oferta y no se han visualizados las facturas correspondientes por la cual se solicito a la empresa ITC S.A. vía nota N° 772/17, las documentaciones correspondientes.

5. INFORME JURIDICO

LOGICALIS PARAGUAY S.A
Verificadas las documentaciones legales requeridas a la oferente se observa que la misma se ajusta sustancialmente a la documentación legal exigida en el Pliego de Bases y Condiciones y lo dispuesto en la Ley N° 2051/03 "DE CONTRATACIONES PÚBLICAS", su Decreto Reglamentario 1107 " POR EL CUAL SE ESTABLECE EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRONICA Y SE DEROGAN LOS DECRETOS N° 12.453/2008 Y 5517/2010

STARK TECNOLOGIA S.A
Verificadas las documentaciones legales requeridas a la oferente se observa que la misma se ajusta sustancialmente a la documentación legal exigida en el Pliego de Bases y Condiciones y lo dispuesto en la Ley N° 2051/03 "DE CONTRATACIONES PÚBLICAS", su Decreto Reglamentario 1107 " POR EL CUAL SE ESTABLECE EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRONICA Y SE DEROGAN LOS DECRETOS N° 12.453/2008 Y 5517/2010

ITC S.A
Verificadas las documentaciones legales requeridas a la oferente se observa que la misma se ajusta sustancialmente a la documentación legal exigida en el Pliego de Bases y Condiciones y lo dispuesto en la Ley N° 2051/03 "DE CONTRATACIONES PÚBLICAS", su Decreto Reglamentario 1107 " POR EL CUAL SE ESTABLECE EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRONICA Y SE DEROGAN LOS DECRETOS N° 12.453/2008 Y 5517/2010

ONE S.A.
Verificadas las documentaciones legales requeridas a la oferente se observa que la misma se ajusta sustancialmente a la documentación legal exigida en el Pliego de Bases y Condiciones y lo dispuesto en la Ley N° 2051/03 "DE CONTRATACIONES PÚBLICAS", su Decreto Reglamentario 1107 " POR EL CUAL SE ESTABLECE EL PROCEDIMIENTO DE SUBASTA A LA BAJA ELECTRONICA Y SE DEROGAN LOS DECRETOS N° 12.453/2008 Y 5517/2010

INSTITUTO DE PREVISION SOCIAL
Lic. Hermógeno Ramón Rivas
DIRECCION GENERAL DE CONTRATACIONES

Miguel Centurión
Dpto. de Telecomunicaciones
Dirección de Informática
Instituto de Previsión Social

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Gonzalez Giret
Oficial de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

6. REGISTRO DE INHABILITADOS

Verificado en la página de la Dirección de Contrataciones Públicas Contrataciones Públicas se puede verificar que las firmas **LOGICALIS PARAGUAY S.A, STARK TECNOLOGIA S.A, ITC S.A y ONE S.A.** se encuentran habilitadas para contratar con el Estado.-

7. VERIFICACION DE LA DOCUMENTACION SUSTANCIAL

N°	Empresa	Formulario de la Oferta		Documentos que acrediten la representación legal del firmante de la oferta		Garantía de Mantenimiento de Oferta		Declaración Jurada Art. 20 inc. "w" y Art. 40 de la Ley 2051/03 (Resolución DNCP N° 330/07)	
		Cumple	No Cumple	Cumple	No Cumple	Cumple	No Cumple	Cumple	No Cumple
1	**LOGICALIS PARAGUAY S.A**	X		X		X		X	
2	**ONE S.A**	X		X		X		X	
3	**STARK TECNOLOGIA S.A.**	X		X		X		X	
4	**ITC S.A.**	X		X		X		X	

8. VERIFICACIÓN DE DOCUMENTOS FORMALES

Documentos legales	LOGICALIS PARAGUAY S.A	STARK TECNOLOGIA S.A	ITC S.A	ONE S.A.
	Cumple/ No Cumple	Cumple/ No Cumple	Cumple/ No Cumple	Cumple/ No Cumple
a. Constancia de inscripción en el Registro Único de Contribuyentes RUC	**Cumple**	**Cumple**	**Cumple**	**Cumple**
b. Documentos de Identidad de los representantes o apoderados de la Sociedad.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
c. Patente Municipal vigente	**Cumple**	**Cumple**	**Cumple**	**Cumple**
d. Declaración Jurada en la que se garantice que el oferente no se encuentra involucrado en prácticas que violen derechos de los menores estipulados en la Constitución Nacional, los Convenios 138 y 182 de la Organización Internacional del Trabajo (OIT), el Código del Trabajo, Código de la Niñez y la Adolescencia, demás leyes y normativas vigentes en la República del Paraguay, conforme al formato aprobado por la Dirección Nacional de Contrataciones Públicas en la Resolución DNCP N° 941/2010.	**Cumple**	**Cumple**	**Cumple**	**Cumple**

INSTITUTO DE PREVISION SOCIAL
Lic. Hernán Ramón Rivas
DIRECCIÓN OPERATIVA DE CONTRATACIONES

Miguel Centurión
Director de Tecnología e Informática
Instituto de Previsión Social

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Caballero Giménez
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicación

e. Fotocopia simple Certificado de Cumplimiento Tributario vigente.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
f. Presentar copias de Contratos y/o Facturas a través de las cuales el oferente demuestre haber facturado en la provisión de Soluciones de Gestión de Identidad y/o Software de Seguridad de Red a Instituciones Públicas o Privadas dentro de los últimos 5 (cinco) años (2011 – 2012 – 2013 – 2014-2015), y que el volumen de negocios en su totalidad sea igual o superior al 50% (cincuenta por ciento) del valor de su oferta. Serán aceptadas referencias de implementación de soluciones de gestión de fabricante y/o integrador de la solución ofertada.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
g. Autorización del fabricante: a) Si el oferente es fabricante del producto que oferta, deberá presentar el documento que lo acredite como tal. b) Si el oferente es Representante o Distribuidor del producto que oferta, deberá presentar la autorización del fabricante c) Si el oferente es Distribuidor del Representante Local del Fabricante, deberá presentar un poder o autorización otorgado por éste último. No obstante, se deberá acompañar copia de la Autorización del Fabricante otorgada al Representante Local. Para b) y el Representante Local, la documentación requerida es el formulario incluido en la Sección VI. Este formulario podrá ser reemplazado por la documentación que pruebe fehacientemente que el oferente es Representante o Distribuidor autorizado del bien que oferta. Asimismo, la documentación podrá ser presentada en copia simple, no obstante, para la firma del Contrato la misma deberá estar inscripta en el Registro Público de Comercio, Sección Representaciones.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
h. Deberá contar en su planilla de Aporte Obrero Patronal del mes anterior a la presentación de la oferta con 1 técnico certificado por el fabricante en la solución ofertada que será el responsable de la ejecución del proyecto. En caso de que el técnico certificado no sea parte del plantel permanente de la empresa oferente, se deberá presentar declaración jurada del mismo por la cual se compromete a firmar un contrato de trabajo para la	**Cumple**	**Cumple**	**Cumple**	**Cumple**

INSTITUTO DE PREVISION SOCIAL
Lic. Herminio Ramón Rivas
DIRECCION OPERATIVA DE LA COMISION DE EVALUACION

Miguel Cantusión
Dpto. de Telecomunicaciones
Dirección de Informática
Instituto de Previsión Social

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Coronel Giménez
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicación

ejecución del proyecto en caso de que la empresa oferente resulte adjudicada. Para la firma del Contrato se deberá presentar el Contrato de Trabajo, que debe extenderse por el tiempo requerido hasta culminar el proyecto, entre el técnico certificado propuesto en la oferta y la empresa adjudicada.				
i. Carta firmada por el fabricante, donde detalle y demuestre como mínimo 3 implementaciones exitosas de solución de gestión de identidad en los últimos 5 años. Deberá proveer información de contacto de la empresa/institución para contactar y realizar las consultas que se consideren necesarias.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
j. Planilla de Precios en planilla Excel en medios magnéticos, versión 2003 o posterior.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
k. Declaración Jurada de conocer el Pliego de Bases y Condiciones y sus Adendas.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
l. Certificado de Cumplimiento Tributario Vigente.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
m. Copia Autenticada Patente Municipal Vigente	**Cumple**	**Cumple**	**Cumple**	**Cumple**
n. Certificado de cumplimiento con el Seguro Social vigente	**Cumple**	**Cumple**	**Cumple**	**Cumple**
o. Balances de los años 2013, 2014 y 2015.	**Cumple**	**Cumple**	**Cumple**	**Cumple**
p. Copia Autenticada del Impuesto a la Renta de los tres últimos años (2013, 2014 y 2015).	**Cumple**	**Cumple**	**Cumple**	**Cumple**
q. Certificado de Origen del servicio ofertado, emitido por el Ministerio de Industria y Comercio para los servicios de origen nacional. Conforme lo establece la ley 4558/11 y el Decreto N° 9649/12que reglamenta la aplicación del Margen de Preferencia. ***La omisión de la presentación del documento correspondiente, no supone la descalificación del oferente, sino simplemente la no aplicación del margen previsto***	**Cumple**	**No Cumple**	**No Cumple**	**Cumple**

INSTITUTO DE PREVISIÓN SOCIAL
Lic. Víctor Corvalán Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

INSTITUTO DE PREVISION SOCIAL
Lic. Herminio Ramón Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

Miguel Centurión
Dpto. de Desarrollo
Dirección de Informática
Instituto de Previsión Social

9. ESPECIFICACIONES TECNICAS

	ESPECIFICACIONES TÉCNICAS	OBS	LOGICALLIS PARAGUAY S.A	STARK TECNOLOGIA S.A	ITC S.A.	ONE S.A.
	1. Descripción General					
	Proveer de una herramienta que permita la Administración y Gobierno de Accesos de Identidades (IAG) permitiendo:		**Cumple**	**Cumple**	**Cumple**	**Cumple**
*	La automatización del proceso de requerir, aprobar, certificar y auditar el acceso a las aplicaciones, datos y otros servicios de TI					
*	La automatización del proceso de entregar información de gobierno y seguridad sobre como las identidades son creadas, administradas y utilizadas para acceder a las aplicaciones.					
	Al automatizar estos procesos la organización espera alcanzar como beneficios:					
*	Cumplir con los requerimientos de cumplimiento de regulaciones y disminuir los riesgos de seguridad					
*	Mejorar la Eficiencia Operativa de estos Procesos de IAG					
	Para automatizar estos procesos y alcanzar los beneficios anteriormente enunciados, se considera que la solución debe poder cumplimentar con las siguientes categorías de funcionalidades de IAG.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
a.-	Evaluación del Estado Actual de IAM					
b.-	Control de Calidad y Limpieza de Privilegios					
c.-	Gobierno de Identidades					
d.-	Administración de Roles					
e.-	Administración & Aprovisionamiento de Usuarios					
f.-	Administración de Requerimientos de Servicios de Accesos					
	2. Alcance					
	Debe contemplar:					
*	La implementación de la solución, que sirva de administrador central, permitiendo una administración centralizada, admitiendo la administración descentralizada por grupos de cuentas de usuarios previamente definidos.		**Cumple**	**Cumple**	**Cumple**	**Cumple**

INSTITUTO DE PREVISION SOCIAL
Lic. Hernán Ramón Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

INSTITUTO DE PREVISION SOCIAL
Lic. Victor Corvalán Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

Miguel Gaona
Director
Dirección de Tecnología de la Información y Comunicaciones
Instituto de Previsión Social

*	La implementación de la solución en un servidor que sirva de administrador central de las cuentas de usuarios.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
*	La administración de, por lo menos, 16.000 cuentas de usuarios activas, con proyecciones de crecimiento, en las distintas plataformas utilizadas por la Institución.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	3. Funcionalidades básicas requeridas					
	3.1 Evaluación del Estado Actual de IAM					
	El primer paso crítico en la implementación de un conjunto de procesos de IAM es comprender cuál es el grado de madurez de la organización y evaluar el estado actual de dichos procesos en la organización de manera a poder determinar las áreas críticas y donde mayor necesidad de establecer un sistema automatizado IAM.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Para lo cual la solución debe permitir realizar un 'GAP Analysis' que permita identificar las aplicaciones y sistemas que serán más beneficiados por una sistematización de los procesos de IAM y que contribuyan a una disminución de los riesgos para la organización		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	La solución en términos generales debería soportar las siguientes áreas:					
	Requerimientos mínimos					
1	Importar datos desde como mínimo 3 de los sistemas más significativos de la organización y poder establecer una comprensión del estado actual de las identidades, roles y estado de privilegios en un período corto de tiempo (5 a 10 días). Se importarán datos de usuarios del ACTIVE Directory (Microsoft), Oracle, MSSQL y se integrarán 4 plataformas adicionales a definir luego del GAP Análisis. En total serían 7 plataformas integradas	Adenda 11	**Cumple**	**Cumple**	**Cumple**	**Cumple**
2	Cuantificar el número de usuarios, grupos, roles y privilegios de los sistemas significativos de la organización		**Cumple**	**Cumple**	**Cumple**	**Cumple**
3	Evaluar la calidad de los privilegios y roles definidos		**Cumple**	**Cumple**	**Cumple**	**Cumple**
4	Identificar y cuantificar: Privilegios excepcionales Asignación inconsistente de permisos Usuarios con permisos de accesos excesivos		**Cumple**	**Cumple**	**Cumple**	**Cumple**
5	Tener la capacidad de evaluar reglas de segregación de funciones que puedan ser utilizadas para evaluar el riesgo para cada rol asignado		**Cumple**	**Cumple**	**Cumple**	**Cumple**
6	Identificar riesgos y necesidades de cumplimiento de regulaciones, así como 'inhibidores' de una implementación de procesos IAM		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	3.2 Control de Calidad y Limpieza de Privilegios					

INSTITUTO DE PREVISION SOCIAL
Lic. Hermilio Ruben Ríos
DIRECCIÓN OPERATIVA DE CONTRATACIONES

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Corvalán Giménez
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

Lic. Miguel Colmán
Dpto. de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones
INSTITUTO DE PREVISION SOCIAL

	La solución ofrecida debe poder determinar cuál es el estado actual de los usuarios y permisos actualmente asignados para tener una evaluación base de la situación actual y poder determinar la estrategia de implementación que sea más conveniente para la organización.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Esto involucra la creación de un repositorio de identidades basado en los datos de las fuentes autoritativas y aplicaciones, correlacionando el acceso y luego identificando permisos fuera de patrón, cuentas huérfanas y usuarios colectores de permisos.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	La solución debe soportar que este sea un proceso iterativo, que permita un refinamiento de los accesos de los usuarios mejorando las políticas y procesos.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Requerimientos mínimos					
1	La solución debe soportar un repositorio de identidades de todas las aplicaciones de TI		**Cumple**	**Cumple**	**Cumple**	**Cumple**
2	La solución debe proveer una visión consolidada de los usuarios, roles y privilegios asociados junto con las uniones entre cada uno de ellos		**Cumple**	**Cumple**	**Cumple**	**Cumple**
3	La solución sería capaz de analizar los sistemas existentes (aun los que no tienen roles definidos) con un nivel de granularidad y análisis que permita identificar temas de seguridad y cumplimiento de regulaciones / auditoría.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
4	La solución debe soportar la importación/exportación de datos de: Usuarios, roles y autorizaciones AD/Windows Windows File Shares UNIX/LINUX Otros tipos de aplicaciones (por ej: Oracle)		**Cumple**	**Cumple**	**Cumple**	**Cumple**
5	La solución debe permitir la importación y administración de datos que sea ejecutada en forma inmediata o planificada a intervalos regulares en forma batch.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
6	La solución debe permitir la importación/exportación de datos vía archivos CSV y LDIF		**Cumple**	**Cumple**	**Cumple**	**Cumple**
7	La solución debe poder identificar automáticamente y remediar las siguientes excepciones a privilegios tales como: Cuentas, roles y recursos Huérfanos Colectores de privilegios excesivos Privilegios fuera de patrón		**Cumple**	**Cumple**	**Cumple**	**Cumple**
8	La solución debe permitir automatizar los procesos de consulta a los propietarios de roles/recursos que validen las excepciones necesarias		**Cumple**	**Cumple**	**Cumple**	**Cumple**
9	La solución debe permitir la generación de reportes en forma simplificada para identificar las excepciones de privilegios		**Cumple**	**Cumple**	**Cumple**	**Cumple**

INSTITUTO DE PREVISION SOCIAL
Lic. Hermitio Ramírez Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

INSTITUTO DE PREVISION SOCIAL
Lic. Victor Corvalán Girt
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

Miguel Centurión
Dirección de Tecnología de la Información y Comunicaciones
Instituto de Previsión Social

	3.3 Gobierno de Identidades					
	La evolución de los requerimientos internos y externos para el cumplimiento de regulaciones, exigen que las organizaciones deben asegurarse que los usuarios solo acceden a los recursos que son necesarios para cumplir su función de trabajo.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Esto se puede lograr combinando las acciones de control proactivo de asignación de permisos en forma preventiva de acuerdo a reglas de segregación de funciones e identificando instancias donde se hayan asignado permisos en forma inapropiada anteriormente.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Por lo cual es necesario que la solución provea los medios para centralizar los controles de cumplimiento de políticas de identidades y automatizar los procesos asociados con el cumplimiento de los controles.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Requerimientos Mínimos					
1	La solución debe permitir definir reglas de negocio/compliance en forma fácil, mediante una interfaz en la que no sea necesario programar		**Cumple**	**Cumple**	**Cumple**	**Cumple**
2	Las reglas de negocio deben permitir especificar controles de: Segregación de Funciones Restricciones de negocio tales como ubicación, función de trabajo, propiedad de datos y otros criterios Políticas entre sistemas Ejecución de transacciones		**Cumple**	**Cumple**	**Cumple**	**Cumple**
3	La solución debe soportar la asignación y monitoreo de riesgos a cualquier combinación de permisos de acceso		**Cumple**	**Cumple**	**Cumple**	**Cumple**
4	La solución debe permitir la asignación de una calificación de riesgo basado en una combinación de condiciones de negocio (ubicación, función, etc.)		**Cumple**	**Cumple**	**Cumple**	**Cumple**
5	La solución debe soportar la asignación y monitoreo de riesgos a cualquier combinación de permisos de acceso		**Cumple**	**Cumple**	**Cumple**	**Cumple**
6	La solución debe permitir la asignación de una calificación de riesgo basado en una combinación de condiciones de negocio (ubicación, función, etc.)		**Cumple**	**Cumple**	**Cumple**	**Cumple**
7	La solución debe permitir la certificación automática para: Usuarios Roles Recursos		**Cumple**	**Cumple**	**Cumple**	**Cumple**

	Identificar las cuentas relevantes y ejecutar certificaciones de solo un subconjunto de dato , por ej: Permisos que violan una política de segregación de funciones Combinaciones de permisos de accesos potencialmente riesgosas basado en análisis de patrones Recursos con 'links' directos a los usuarios (opuesto al modelo de roles) Cuentas Huérfanas Permisos que cambian entre fechas		**Cumple**	**Cumple**	**Cumple**	**Cumple**
9	La solución debe alertar a los usuarios de violaciones a las políticas durante el contexto de una campaña de certificación		**Cumple**	**Cumple**	**Cumple**	**Cumple**
10	La solución debe permitir integrarse con los sistemas de aprovisionamiento para una remediación automática		**Cumple**	**Cumple**	**Cumple**	**Cumple**
11	La solución debe mostrar mediante reportes y tableros de control el estado de cumplimiento de la organización		**Cumple**	**Cumple**	**Cumple**	**Cumple**
12	Las políticas de compliance deben poder evaluar los privilegios de acceso entre múltiples sistemas. Por ej: Que un usuario que tiene un privilegio no tenga otro determinado privilegio en LINUX		**Cumple**	**Cumple**	**Cumple**	**Cumple**
13	Brindar la facilidad que los administradores especifiquen en forma automatizada el lanzamiento de correos de recordatorio y alertas		**Cumple**	**Cumple**	**Cumple**	**Cumple**
14	Brindar la facilidad que los administradores requieran la justificación mediante un comentario de la certificación de acceso de un usuario que está violando una política de cumplimiento		**Cumple**	**Cumple**	**Cumple**	**Cumple**
15	Brindar la facilidad que los gerentes de negocio puedan certificar el acceso de los usuarios en forma amigable Por favor ejemplifique un proceso de certificación		**Cumple**	**Cumple**	**Cumple**	**Cumple**
16	Brindar la facilidad que el motor de cumplimiento de políticas pueda ser integrado a otros sistemas mediante 'web services' (por ejemplo : sistemas de aprovisionamiento y mesas de ayuda)		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	3.4 Administración de Roles					
	Una buena definición de roles tiene un impacto directo en la complejidad y dificultad de los procesos de aprovisionamiento de usuarios debido a la cantidad de roles a implementar y políticas de asignación de permisos e identidades a definir para adecuarse a la necesidad que necesita la organización.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Un buen modelo de roles brinda el contexto de negocio que hace que los procesos asociados a la administración de identidades sean comprensibles por el área de negocios		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Requerimientos Mínimos					

	La solución debe permitir el descubrimiento de roles usando técnicas eficientes y rápidas (por ej : usando análisis basado en patrones) Brinde ejemplos de experiencias de descubrimiento de roles en clientes.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
2	La solución debe permitir técnicas combinadas según un enfoque 'top-down', 'bottom-up' e hibrido		**Cumple**	**Cumple**	**Cumple**	**Cumple**
3	La solución debe proveer metodologías de descubrimiento de roles 'out-of-the-box' fácilmente customizables mediante parámetros		**Cumple**	**Cumple**	**Cumple**	**Cumple**
4	El descubrimiento de los roles se puede basar en: Atributos de RRHH (departamento, locación, etc.) Combinación de atributos de RRHH Patrones existentes entre los usuarios y privilegios actualmente definidos		**Cumple**	**Cumple**	**Cumple**	**Cumple**
5	La solución debe permitir visualizar en forma fácil los diferentes tipos de asociaciones existentes entre usuarios, roles y recursos.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
6	La solución debe poder asociar los resultados de las diferentes metodologías de descubrimiento de roles utilizadas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
7	La solución debe proveer de reportes que muestren el grado de cubrimiento de permisos de acceso.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
8	La solución debe soportar simulaciones tipo 'what if' para los cambios de roles propuestos.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
9	La solución debe tener la capacidad de trabajar en un ciclo cerrado con los sistemas de: Gestión de Identidades Gestión de Mesa de Ayuda		**Cumple**	**Cumple**	**Cumple**	**Cumple**
10	La solución debe ser escalable y otorgar permisos de accesos a 16 mil usuarios como mínimo.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
11	La solución debe brindar una administración basada en web que se pueda integrar al workflow de la solución		**Cumple**	**Cumple**	**Cumple**	**Cumple**
12	La solución debe poder detectar cambios de permisos de acceso a nivel negocio que requieran cambios en el modelo de roles Por ej: Si se agregan 10 usuarios a un Nuevo rol X y resulta que el rol X es similar al rol Y ya definido, el sistema debe ser capaz de detectar las similitudes y asistir al administrador en resolver las redundancias y reutilizar los roles.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
13	La solución debe permitir automatizar los procesos de negocio para aprobación de roles, autoservicio de roles y modificación de roles		**Cumple**	**Cumple**	**Cumple**	**Cumple**
14	La solución debe poder exponer via web services al motor analítico de roles para interactuar con otras aplicaciones		**Cumple**	**Cumple**	**Cumple**	**Cumple**

INSTITUTO DE PREVISION SOCIAL
Lic. Victor Corvalán Giret
Oficina de Seguridad Informática
INSTITUTO DE PREVISION SOCIAL
Lic. Hermino Ramón Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

Miguel Contreras
Instituto de Previsión Social

	La solución debe permitir la exploración y la importación de cuentas y roles en los siguientes endpoints : Active Directory. Linux. Exchange. Oracle /MS SQL		**Cumple**	**Cumple**	**Cumple**	**Cumple**
16	La solución deber permitir consultas y reportes sobre los permisos de acceso y/o roles que hayan sido asignados a un usuario		**Cumple**	**Cumple**	**Cumple**	**Cumple**
17	La solución deber permitir consultas y reportes sobre los usuarios/roles que tengan un acceso asignado a un recurso especifico o a un permiso de acceso.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
18	La solución debe proveer reportes de privilegios /roles y certificaciones: Certificación de Privilegios de Usuarios Campaña de Certificación de Usuarios Campaña de Certificación de Roles Campaña de Certificación de Recursos Estado de Avance de Certificaciones Requerimientos de Cambios de Privilegios de Usuarios Recertificaciones de Privilegios de Usuarios		**Cumple**	**Cumple**	**Cumple**	**Cumple**
19	La solución debe poder mostrar en un tablero de control el estado en que se encuentran las certificaciones		**Cumple**	**Cumple**	**Cumple**	**Cumple**
20	La solución debe poder mostrar el estado en que se encuentran el cumplimiento de al menos una de las siguientes normas SOX , BASEL y PCI	Adenda 11	**Cumple**	**Cumple**	**Cumple**	**Cumple**
21	La solución debe poder mostrar el estado en que se encuentran los riesgos de la organización La solución debe brindar reportes de Segregación de funciones que permitan: Restricciones entre Grupos Restricciones entre Recursos Restricciones entre Roles Restricciones entre datos de RH y Grupos Restricciones entre Grupos y Recursos		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	3.5 Administración de Usuarios					

	La solución ofrecida debe minimizar la complejidad de la administración de identidades automatizando los procesos de creación, modificación, remoción, o borrado de cuentas en una forma eficiente y confiable. Asimismo, es de gran importancia que la solución ofrecida brinde facilidades que permitan la configuración de políticas y conectores en forma simple y rápida sin necesidad de programar ni de tener que soportar una gran carga de mantenimiento y desarrollo. Deben contar con conectores/adaptadores nativos para las plataformas más conocidas como Microsoft, Oracle, SAP, Linux, etc. y además poseer un framework de desarrollo, que ya cuenta con las funcionalidades y conectores para la generación del adaptador, para plataformas que no se encuentren soportados en forma nativa.	Adenda 11	**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Asimismo, es de gran importancia que la solución ofrecida brinde facilidades que permitan la configuración de políticas y conectores en forma simple y rápida sin necesidad de programar ni de tener que soportar una gran carga de mantenimiento y desarrollo.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Requerimientos Mínimos					
1	Crear, actualizar y eliminar cuentas de usuario en cualquier entorno de la empresa, incluidos sistemas y aplicaciones legados o basados en web		**Cumple**	**Cumple**	**Cumple**	**Cumple**
2	Permitir el almacenamiento de cuentas administradas por la solución en un directorio corporativo		**Cumple**	**Cumple**	**Cumple**	**Cumple**
3	Permitir la definición de una identificación de usuario global (UID global) que permita la asociación y mapeo de Identidades de usuarios a través de distintos 'endpoints' y fuentes autoritativas en base a reglas prestablecidas (Funcionalidad de Autodescubrimiento y correlación de cuentas de usuario)		**Cumple**	**Cumple**	**Cumple**	**Cumple**
4	Soportar la Administración de Identidades para los siguientes tipos de comunidades de usuarios: Empleados Contratados Socios de negocio Usuarios externos (consumidores)		**Cumple**	**Cumple**	**Cumple**	**Cumple**
5	Poder escalar a nivel de Administración y según el tipo de comunidad de usuarios tanto internos como externos.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
6	Permitir delegación granular en forma temporal con: fecha de comienzo de la delegación fecha de finalización de la delegación		**Cumple**	**Cumple**	**Cumple**	**Cumple**
7	Permitir la delegación dinámica de una tarea de aprobación de manera tal de reasignar la tarea a otro usuario dinámicamente según reglas preestablecidas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**

	Permitir cargar en forma masiva la información de usuarios desde más de una fuente autoritativa al mismo tiempo. RRHH propio Oracle		**Cumple**	**Cumple**	**Cumple**	**Cumple**
9	Permitir la carga masiva de usuarios aplicando reglas y realizando transformaciones de datos para normalizar el modelo de datos de usuarios y aplicaciones administradas		**Cumple**	**Cumple**	**Cumple**	**Cumple**
10	Permitir el aprovisionamiento de Usuarios basado en Roles (RBAC): Role Based Access Control.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
11	Permitir que el modelo RBAC de administración de roles también soporte la capacidad de manejar roles anidados		**Cumple**	**Cumple**	**Cumple**	**Cumple**
12	Permitir el aprovisionamiento basado en reglas dinámicas (ABAC: Attribute Based Access Control) de manera de poder realizar la asignación de permisos basado en atributos del usuario.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Sistemas Operativos tales como : Windows 20xx UNIX/Linux		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Bases de Datos que incluyan aplicaciones tales como: SQL Oracle		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Groupware que incluyan aplicaciones tales como: MS Exchange MS Lync		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Servicios de Directorios tales como: Active Directory LDAP genérico		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Sistemas de control de acceso remoto (VPN) como: Kerberos RSA ID y PKI		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Entornos basados en la Nube soportando aplicaciones SaaS tales como: Google Apps Office 365		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Aplicaciones Web que soporten el standard SCIM (System for Cross-domain Identity Management) tales como: Service Now Microsoft Azure Zendesk		**Cumple**	**Cumple**	**Cumple**	**Cumple**
14	Aprovisionar activos físicos tales como: Computadoras		**Cumple**	**Cumple**	**Cumple**	**Cumple**

	Flexibilidad de aprovisionar usuarios de fuentes de identidades donde no tenga un conector. Donde se requiera un aprovisionamiento manual, pueda, a través de un flujo de trabajo, generarse una orden de trabajo, para la creación manual de dicha cuenta a la plataforma solicitada. Una vez finalizada la creación manual, se deberá finalizar el flujo en la herramienta del AIM, para que dicho aprovisionamiento quede registrado en la persona y los reportes del ciclo de vida del usuario.	Adenda 11	**Cumple**	**Cumple**	**Cumple**	**Cumple**
16	Permitir la construcción de conectores a aplicaciones internas o comerciales no soportadas por un conector 'out of the box'. Describir los métodos de integración que brinda la solución a nivel de usuarios y permisos con: Aplicaciones basadas en base de datos Aplicaciones basadas en directorios LDAP Aplicaciones basadas en archivos planos Aplicaciones accesibles via 'web services' Aplicaciones basadas en la Nube		**Cumple**	**Cumple**	**Cumple**	**Cumple**
17	Simplificar el desarrollo de conectores mediante herramientas tipo 'wizard', evitando la necesidad de programar en Java o C++,para aplicaciones que definen usuarios y permisos en: Directorios LDAP (JNDI) Bases de datos RDMBS (ODBC/JDBC) Aplicaciones que exponen su estructura de usuarios y permisos via 'web services'		**Cumple**	**Cumple**	**Cumple**	**Cumple**
18	Soportar una integración a los diferentes sistemas en forma 'agentless' es decir sin necesidad de instalar agentes en los endpoints administrados.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
19	Soportar interfaces a sistemas abiertos como: SPML Web Services APIs Java		**Cumple**	**Cumple**	**Cumple**	**Cumple**
20	La solución debe permitir el diseño y especificación de los workflows en forma gráfica, sin necesidad de programar en lenguaje de scripting para poder definir los workflows		**Cumple**	**Cumple**	**Cumple**	**Cumple**
21	Tener la capacidad de cambiar el camino de aprobación teniendo en cuenta en el resultado de los pasos intermedios basado en reglas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
22	La solución debe soportar las normas estándares de la industria para especificación de Workflow. (Standard WfMC) para permitir la comunicación otros workflows que soporten dichos estándares.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
23	La solución debe proveer modelos de ejemplo de workflows de aprobación preconfigurados que aceleren la implementación de la solución		**Cumple**	**Cumple**	**Cumple**	**Cumple**

24	Permitir Workflows de aprobación: En serie En Paralelo Teniendo X de Y cantidad de Aprobaciones		**Cumple**	**Cumple**	**Cumple**	**Cumple**
25	Permitir la integración con terceras partes via Web Services (WDSL y SOAP) exponiendo las tareas de Administración de Identidades para poder ser integradas con otras aplicaciones		**Cumple**	**Cumple**	**Cumple**	**Cumple**
26	Proveer un modelo de escalamiento de aprobaciones por tiempo		**Cumple**	**Cumple**	**Cumple**	**Cumple**
27	Permitir formular Políticas de Identidades basadas en lógica de negocio que permitan la ejecución de cambios de negocio cuando se cumple una condición o se evalúa una regla determinada: Los cambios de negocios pueden ser: Asignar o revocar roles Asignar o revocar membresías de grupos Actualizar atributos de un perfil de usuario		**Cumple**	**Cumple**	**Cumple**	**Cumple**
28	Permitir que una política de identidades se aplique en forma selectiva a un grupo de usuarios determinados, de manera de evitar que todo el universo de usuarios y solo se aplique a un 10 % de usuarios solamente.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
29	Permitir formular Políticas de Identidades Preventivas que eviten que un usuario reciba privilegios. Estas políticas deben ser ejecutadas antes que la tarea de aprovisionamiento sea ejecutada, permitiendo que el administrador chequee las violaciones a las políticas antes de asignar o cambiar atributos de un perfil, si existe una violación el administrador puede limpiar la violación antes de submitir la tarea		**Cumple**	**Cumple**	**Cumple**	**Cumple**
30	Permitir la construcción de Políticas de Identidades complejas sin necesidad de programar en Java o C++, mediante una herramienta tipo 'Wizard'.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
31	Tener la capacidad de sincronizar cuentas: Hacia Afuera: Desde la definición central de la organización en el sistema de Adm. de Identidades a los sistemas administrados a través de políticas de identidades y roles. Hacia Adentro: Desde los sistemas administrados hacia el sistema de Adm. de Identidades detectando cambios a través de un proceso de sincronización reversa		**Cumple**	**Cumple**	**Cumple**	**Cumple**

32	Poder realizar una sincronización reversa detectando cualquier tipo de cambio realizados en forma directa en los 'endpoints' por fuera del proceso normal de Adm. de Identidades tales como creación de cuentas nuevas, atributos modificados, etc. La detección de cambios realizados por afuera de la herramienta de Adm. de Identidades debe poder ejecutar las acciones siguientes: Aceptar Borrar Suspender Enviar a flujo de aprobación, etc.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
33	Poder realizar la sincronización de usuarios del Active Directory Server (ADS), con información de usuarios de aplicaciones en la nube. Por ejemplo: se puede configurar para que el ADS sincronice adiciones o cambios del grupo local y lo propague al entorno de nube.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
34	Tener la capacidad para gestionar las altas y bajas de cuentas en forma mediante la lectura de archivos csv o txt La carga masiva de usuarios debe permitir: a) Transformar datos antes de cargarlos b) Ejecutar un workflow que permita realizar las acciones siguientes a nivel de ABM de usuario: Aprobar Rechazar Reservar Liberar		**Cumple**	**Cumple**	**Cumple**	**Cumple**
35	La solución debe poder modificar en forma masiva los atributos de un usuario basado en: Un atributo filtro, tal como departamento, ciudad, fecha de ingreso, fecha de egreso etc. Por ej.: Se quiere modificar todos los usuarios que pertenecen a un departamento determinado.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
36	La solución debe permitir la notificación de correos electrónicos basado en Políticas, es decir que basado en la información del evento y/o de la fecha , se configurará dinámicamente el cuerpo del mensaje, el remitente y el receptor		**Cumple**	**Cumple**	**Cumple**	**Cumple**
37	Mostrar en forma online las modificaciones realizadas por los administradores directamente desde la Consola de las Aplicaciones, por fuera del proceso normal de Adm. de Identidades tales como creación de cuentas nuevas, atributos modificados, etc.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
38	Tener la capacidad para programar las altas y bajas de cuentas basadas en un calendario de tiempo, con una fecha efectiva de arranque y fecha efectiva de terminación		**Cumple**	**Cumple**	**Cumple**	**Cumple**
39	Tener la capacidad de buscar usuarios en el directorio basado en diferentes atributos de usuarios tales como ID de usuario, apellido, primer nombre, etc. Esta capacidad que generalmente tienen los administradores debe poder ser delegada a los usuarios finales (i.e., funcionalidad de 'páginas blancas')		**Cumple**	**Cumple**	**Cumple**	**Cumple**

40	Los usuarios deberán poder ver la información con filtros de acuerdo a su rol, de manera que un usuario final pueda ver su nombre y apellido, oficina, teléfono y dirección, mientras que el gerente del mismo vea además sus roles		**Cumple**	**Cumple**	**Cumple**	**Cumple**
41	Tener la capacidad de definir un ID de usuario único durante la creación de la cuenta de una identidad en el 'endpoint' basada en una lógica predefinida que debe considerar las siguientes situaciones de conflicto: a) Que el usuario este previamente definido en cuyo caso deberá generar una ID de usuario única b) Que el usuario haya sido retirado o deshabilitado en cuyo caso se deberá prevenir la reutilización del mismo usuario.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
42	La solución debe tener una administración web online de los endpoints administrados que permita: Manejar multiples endpoints desde un único lugar (tanto predefinidos como dinámicos) Manejar multiples cuentas, grupos y atributos de conectores dinámicos definidos 'adhoc' por el usuario Tener un control granular de relaciones entre cuentas y grupos Explorar los contenidos de un endpoint, correlacionar las cuentas Definir tipos de endpoints		**Cumple**	**Cumple**	**Cumple**	**Cumple**
43	La solución debe proveer flexibilidad en la administración de permisos, permitiendo un control granular de cambios a nivel de: Roles de negocio Cambios en las cuentas Cambios en los atributos de las cuentas Cambios en los valores de los atributos de las cuentas		**Cumple**	**Cumple**	**Cumple**	**Cumple**
44	La solución debe permitir ver en forma gráfica el estado de la ejecución de los workflows, mostrando el flujo de ejecución a nivel de: Tareas aprobadas Tareas submitidas		**Cumple**	**Cumple**	**Cumple**	**Cumple**
45	La interfaz del usuario y las pantallas de ayuda de la Consola de Usuario de la solución de Administración de Identidades debe poder ser localizada en lenguajes español e inglés.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
46	La interfaz del usuario debe poder ser customizada en forma simple y fácil, permitiendo a la organización cambiar la estructura de las ´páginas (encabezamiento, pie de página), pantallas de ayuda en contexto, etc.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
47	La interfaz del usuario debe poder ser customizada en forma simple y fácil, permitiendo diferentes 'skins' de acuerdo al tipo de usuarios que este ingresando a la interfaz, etc.		**Cumple**	**Cumple**	**Cumple**	**Cumple**

48	La solución debe permitir la aprobación de tareas de flujos de trabajo desde una aplicación disponible en un dispositivo móvil.		Cumple	Cumple	Cumple	Cumple
	3.6 Administración de Requerimientos de Servicios de Acceso					
	La solución ofrecida debe simplificar la operatoria de Administración de Identidades, permitiendo que los usuarios finales sin necesidad de un conocimiento técnico profundo, puedan resolver los temas relacionados con el manejo de sus Identidades y permisos asociados a través de actividades tales como:		Cumple	Cumple	Cumple	Cumple
1	Autoservicio de Registración y Administración de Usuarios		Cumple	Cumple	Cumple	Cumple
2	Autoservicio de Reseteo de Contraseñas		Cumple	Cumple	Cumple	Cumple
3	Administración de Requerimientos de Servicios de Acceso		Cumple	Cumple	Cumple	Cumple
	3.6.1 Autoservicio de Registración y Administración para Usuarios					
1	La solución debe tener la capacidad de permitir el autoservicio de registración y administración de usuarios finales.		Cumple	Cumple	Cumple	Cumple
2	La solución debe proveer una interfaz web que permita a los usuarios de negocio: Actualizar elementos de su Perfil de Usuario Administrar sus contraseñas y configurar las preguntas y respuestas de verificación de identidad Requerir el acceso a: A un rol o permiso A un servicio de negocio o aplicación A la creación de un nuevo rol		Cumple	Cumple	Cumple	Cumple
3	Permitir que un usuario final pueda visualizar el estado de los requerimientos que realizó		Cumple	Cumple	Cumple	Cumple
4	Permitir que un usuario final pueda ver los roles asignados así mismo, y dependiendo de cómo este configurado ver roles que pueden delegar a otras personas		Cumple	Cumple	Cumple	Cumple
5	Permitir que el proceso de registración obligue al usuario final a dar como leída y aceptada, las condiciones de acceso a la organización, pudiendo ser un formulario de aceptación o una política de seguridad global aprobada.		Cumple	Cumple	Cumple	Cumple
6	Permitir que el proceso de registración permita establecer diferentes métodos de verificación de identidad: Validación de Respuestas a los atributos ingresados en la pantalla de registración que son validados via web services contra sistemas internos/externos de validación Validación del usuario en forma posterior por parte de un administrativo		Cumple	Cumple	Cumple	Cumple
7	La solución debe proveer formularios HTML prearmados para la registración de usuarios.		Cumple	Cumple	Cumple	Cumple
8	La solución debe proveer un servicio de Identificación de Usuario Olvidada que permite mediante un desafío de preguntas/respuestas recuperar la información de usuario.		Cumple	Cumple	Cumple	Cumple

	3.6.2 Autoservicio de Reseteo de Contraseñas					
1	La solución debe permitir que los usuarios autogestionen sus contraseñas a través de la consola WEB de la solución.		Cumple	Cumple	Cumple	Cumple
2	La solución debe tener un sistema de administración de contraseñas flexible que permite establecer políticas fuertes de: Composición Reutilización Expiración Reseteo Autoservicio Propagación Sincronización Integración		Cumple	Cumple	Cumple	Cumple
3	Permitir asignar a un usuario la contraseña por primera vez y luego pedir que la cambie con la primera sesión inicial		Cumple	Cumple	Cumple	Cumple
4	Permitir soportar políticas de composición de contraseña basado en un diccionario de contraseñas no permitidas.		Cumple	Cumple	Cumple	Cumple
5	La solución debe permitir limitar la cantidad de veces que se intenta resetear una contraseña.		Cumple	Cumple	Cumple	Cumple
6	La solución debe brindar un mecanismo de preguntas variables para validar la autenticación		Cumple	Cumple	Cumple	Cumple
7	La solución debe proveer un mecanismo de Autoservicio para que los usuarios puedan ingresar sus propias preguntas de validación de autenticación		Cumple	Cumple	Cumple	Cumple
8	La solución debe permitir soportar políticas de reutilización flexibles y debe permitir guardar la información de las contraseñas utilizadas para evitar su uso recurrente basadas en: Datos de los atributos del perfil de usuario Contraseñas del Diccionario Cantidad mínima de días antes de reusar una contraseña Cantidad mínima de contraseñas antes de volver a reusar la contraseña Porcentaje de diferencia con respecto a la contraseña anterior		Cumple	Cumple	Cumple	Cumple
9	La solución debe permitir soportar diferentes políticas de contraseñas para diferentes grupos de usuarios		Cumple	Cumple	Cumple	Cumple
10	La solución debe permitir soportar políticas de expiración de contraseñas flexibles para satisfacer las necesidades de la organización, basadas en: Inactividad de un usuario (seguimiento de logins exitosos) Cantidad de contraseñas incorrectas (seguimiento de logins fallidos)		Cumple	Cumple	Cumple	Cumple

11	La solución debe proveer un mecanismo de propagación de cambio de contraseñas a todas las plataformas soportadas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
12	La solución debe brindar un mecanismo para atrapar cambios de contraseñas cuando se realizan puntualmente en los 'endpoints' y sincronizar en forma bidireccional estos cambios con la solución de Administración de Identidades. Plataformas soportadas: AD (Windows) Unix /Linux LDAP		**Cumple**	**Cumple**	**Cumple**	**Cumple**
13	La solución debe proveer servicios de password olvidado o reseteo de password soportando la integración de los servicios de contraseñas de la herramienta con el login de Windows.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
14	La solución debe contar con una aplicación móvil que permita desde un dispositivo móvil (Smartphone) realizar las tareas siguientes: Reseteo de Contraseñas Cambio de Contraseñas Responder a solicitudes de aprobación Visualización de información a nivel gerencial para aprobar Nota: Como mínimo debe soportar IOS y Android		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	3.6.3 Administración de Requerimientos de Servicios de Acceso					
1	La solución debe presentar una interfaz intuitiva a nivel usuario final que simplifique el proceso de requerimiento de acceso a través de un tipo de 'carrito de compras' donde los usuarios puedan seleccionar los roles y permisos que sean necesarios para cumplir sus funciones		**Cumple**	**Cumple**	**Cumple**	**Cumple**
2	La solución debe permitir que el usuario final pueda visualizar: Detalles de Perfil de Usuario Acceso Actual Cuentas asignadas para cada usuario Capacidad de realizar acciones permitidas tales como: Bloqueo/Desbloqueo, Suspensión, Reseteo de Contraseñas Estado de sus Requerimientos de Acces , y Certificaciones de Acceso		**Cumple**	**Cumple**	**Cumple**	**Cumple**
3	La solución debe permitir que el usuario final pueda visualizar y hacer un seguimiento activo del proceso de solicitud de acceso siguiendo una línea de tiempo (cuando fue pedido, cuando fue aprobado, que queda pendiente).		**Cumple**	**Cumple**	**Cumple**	**Cumple**
4	La solución debe permitir el manejo de un Catálogo de permisos granulares de manera tal que permita solicitar: Roles Membresía de grupos		**Cumple**	**Cumple**	**Cumple**	**Cumple**

	Atributos de usuario					
5	La solución debe soportar un Modelo de Permisos que permita presentar y agrupar los mismos en forma lógica de manera que el usuario final pueda navegar fácilmente para solicitar los permisos que necesita. Las agrupaciones lógicas deberían ser al menos las siguientes: Aplicaciones Grupo de Aplicaciones Roles Grupo de Roles Permisos de Negocio		**Cumple**	**Cumple**	**Cumple**	**Cumple**
6	La solución la aceptación o rechazo de un requerimiento de acceso basado en una evaluación de riesgo entre el permiso solicitado y los permisos existentes.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	4. Etapas del Proyecto – Tareas a Ejecutar					
	Etapa I: Etapa Inicial					
	1.- Instalación y configuración de la solución – contemplar un esquema clusterizado	Adenda 11				
	2.- Administración de Usuarios					
	a.- Relevamiento					
	Tareas de relevamiento que permita conocer toda la variedad de los ámbitos funcionales y organizacionales de la Institución, determinando los niveles de usuarios existentes y proyectados.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	b.- Definición de Esquema de Políticas de Acceso					
	Definición de esquema de políticas de acceso conforme a la estructura organizacional existente. Esta definición debe estar diseñada de forma tal que permita la flexibilidad ante cambios de estructuras organizacionales que pudiera presentarse, de manera que estos puedan aplicarse de una manera simple y sencilla, minimizando el impacto que pueda producir.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	c.- Definición de Roles					
	La definición de roles y sus privilegios será en bases al esquema de políticas de acceso definida, manteniendo la flexibilidad de cambios que puedan producirse y apuntando al nivel mínimo de granularidad.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	d.- Definición de Usuarios "Especiales"					

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Corvalán Giret
Oficina de Seguridad Informática
INSTITUTO DE PREVISION SOCIAL
Lic. Hermindo Ramírez Rivas
Dirección de Tecnología de la Información y Comunicaciones
DIRECCION OPERATIVA DE CONTRATACIONES
Miguel Cañarián
Instituto de Previsión Social

Se definirán los roles y los privilegios de los usuarios que requieren accesos especiales a ciertos recursos tecnológicos, en razón de sus funciones como especialistas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
- Plan de Acción					
Conforme al diagnóstico obtenido en el punto anterior, se elaborará un Plan de Acción, que deberá incluir niveles de prioridad para la implementación, recursos necesarios, plazos esperados, e incluir los siguientes aspectos: 3.1 Desarrollo 3.2 Pruebas 3.3 Implementación 3.4 Capacitación		**Cumple**	**Cumple**	**Cumple**	**Cumple**
Una vez finalizadas las tareas y presentados los documentos requeridos en esta etapa en forma satisfactoria conforme a los requerimientos exigidos, **se emitirá un Acta de Conformidad por la Etapa Inicial.**		**Cumple**	**Cumple**	**Cumple**	**Cumple**
Etapa II: Implementación					
A. Desarrollo					
El desarrollo comprende todas las modificaciones que deba realizarse a los productos para ajustarlos a las necesidades de la Institución, incluso las referentes al idioma.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
B. Pruebas					
Las pruebas serán realizadas en un servidor instalado en la Institución y bajo supervisión del personal técnico designado por la misma, tomando un ámbito que pueda servir de Plan Piloto.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
C. Implementación					
La implementación será realizada en el servidor de producción instalado en la Institución y bajo supervisión del personal técnico designado por la misma respetando las políticas de seguridad implementadas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
D. Capacitación					
Se deberá prever la capacitación en la Administración de la Plataforma para 5 personas, con una carga mínima de 40 hs en las oficinas que el IPS disponga. Así también, los trabajos para la solución de cualquier evento que surja durante el soporte técnico, deberá tener el acompañamiento de técnicos designados por el IPS.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
E.- Entrega de Informes					

	1.- Informes del resultado de las implementaciones					
	2.- Manuales					
	a.- Técnico					
	Debe contemplar todas las informaciones técnicas necesarias, para que el personal designado por la Institución, pueda realizar monitoreo de comportamiento de las bases de datos y obtención de información especializada.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	b.- Operativo					
	Debe contemplar todas las opciones implementadas y que permita al personal operativo, sea cual fuere el nivel, contar con un material de apoyo para realizar sus operaciones cotidianas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Una vez finalizadas las tareas y presentados los documentos requeridos en esta etapa en forma satisfactoria conforme a los requerimientos exigidos, se emitirá un Acta de Conformidad por la Etapa de Implementación.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Etapa III: Soporte Técnico					
	Incluye los siguientes servicios:					
1	Soporte presencial o remoto por implementación será de un máximo de 20 horas mensuales, durante toda la vigencia del contrato, de lunes a viernes en el horario de 8 a 16 hs con 4 horas de respuesta como máximo, (vía telefónica, correo electrónico, chat, web, o similar).	Adenda 11	**Cumple**	**Cumple**	**Cumple**	**Cumple**
2	Resumen mensual del estado de implementación		**Cumple**	**Cumple**	**Cumple**	**Cumple**
3	Informe mensual de la asistencia realizada.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Una vez finalizado el plazo del soporte técnico requerido, y de haberse cumplido el miso de forma satisfactoria, se emitirá un Acta de Conformidad por el Soporte Técnico.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	5. Confidencialidad					
	El oferente deberá proteger la información obtenida durante el desarrollo del trabajo, haciéndose responsable por cualquier daño/perjuicio que se pudiera ocasionar por el uso indebido de la información accedida.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	El oferente consignará un Acuerdo de Confidencialidad que obligará, entre otras cosas:		**Cumple**	**Cumple**	**Cumple**	**Cumple**
a.-	Mantener el carácter secreto de la Información Confidencial y no darla a conocer sin el consentimiento escrito de la Institución.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
b.-	Utilizar la Información Confidencial exclusivamente para las tareas definidas en el alcance específico de este proyecto.		**Cumple**	**Cumple**	**Cumple**	**Cumple**

c.-	Restituir toda la Información Confidencial al solo requerimiento de la Institución. Alternativamente, podrá destruir la Información Confidencial con el consentimiento de la Institución, en cuyo caso deberá probar a ésta tal destrucción.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
d.-	Revelar la Información Confidencial sólo a aquéllas personas cuyo conocimiento sea indispensable para el fin para el cual fue provista. Estas personas tendrán las obligaciones aquí previstas, y el Oferente responderá por ellas.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
e.-	Eliminar toda copia electrónica y/o impresa de la Información Confidencial de cualquiera de los equipos informáticos u otros soportes, salvo autorización de la Institución, una vez finalizado el trabajo.		**Cumple**	**Cumple**	**Cumple**	**Cumple**
	6. Plan de Ejecución:					
La Orden de Servicio será emitida dentro de los 15 días posteriores a la suscripción del Contrato. El Proyecto deberá realizarse en forma conjunta con el Personal Técnico designado por el IPS y cada etapa de la misma deberá ejecutarse conforme a los siguientes plazos:			**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Etapa I : Etapa Inicial					
	Plazo Máximo: 90 días corridos a partir de la recepción de la Orden de Servicio.	Adenda 16	**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Etapa II: Implementación:	Adenda 16	**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Plazo Máximo: 120 días corridos a partir de la emisión del Acta de Conformidad por la Etapa Inicial.	Adenda 16	**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Etapa III. Soporte Técnico:	Adenda 16	**Cumple**	**Cumple**	**Cumple**	**Cumple**
	Esta etapa inicia a partir de la fecha de emisión del Acta de Conformidad por la Etapa de implementación y se extenderá por 20 meses. El soporte presencial o remoto por implementación será de un máximo de 20 horas mensuales, durante toda la vigencia del Contrato, de lunes a viernes en el horario de 8 a 16 hs con 4 horas de respuesta como máximo, (vía telefónica, correo electrónico, chat, web o similar) OBS.: El plazo total de ejecución es de 27 meses incluido el soporte técnico posterior a la implementación.	Adenda 16	**Cumple**	**Cumple**	**Cumple**	**Cumple**

10. CUADRO COMPARATIVO DE PRECIOS:

OFERENTES	ITEM	CODIGO DE CATÁLOGO	DESCRIPCIÓN DEL BIEN	UNIDAD DE MEDIDA	PRESENTACIÓN	CANTIDAD	MARCA	PROCEDENCIA	PRECIO UNITARIO C/IVA	PRECIO TOTAL C/IVA	PRECIO UNITARIO REFERENCIAL	% DE VARIACION
ONE S.A	1	43232402-003	Software de Gestion de Identidad	UNIDAD	UNIDAD	1	CA	USA	2.200.790.526	2.200.790.526	3.526.816.000	-38%
STARK TECNOLOGIA S.A.	1	43232402-003	Software de Gestion de Identidad	UNIDAD	UNIDAD	1	IBM	USA	3.119.000.000	3.119.000.000	3.526.816.000	-12%
ITC S.A.	1	43232402-003	Software de Gestion de Identidad	UNIDAD	UNIDAD	1	RSA	USA	3.526.816.000	3.526.816.000	3.526.816.000	0%
LOGICALIS PARAGUAY S.A	1	43232402-003	Software de Gestion de Identidad	UNIDAD	UNIDAD	1	RSA	EEUU	4.200.000.000	4.200.000.000	3.526.816.000	19%

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Corvalán Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

INSTITUTO DE PREVISION SOCIAL
Lic. Herminio Palacios Rivas
DIRECCIÓN OPERATIVA DE CONTRATACIONES

Miguel Centurión
Depto. de Tecnología
Dirección de Informática
Instituto de Previsión Social

11. CAPACIDAD FINANCIERA

Empresa:		ONE S.A.							
		2013		2014		2015		Promedio	Observaciones
Ratio de Liquidez	Activo corriente	1.135.721.499	2,34	2.156.604.488	2,68	3.529.245.223	4,11	3,04	CUMPLE
	Pasivo corriente	485.722.459		802.777.069		858.736.274			
Endeudamiento	Pasivo total	485.722.459	0,39	802.777.069	0,35	858.736.274	0,23	0,33	CUMPLE
	Activo total	1.229.887.932		2.271.793.105		3.669.561.669			
Rentabilidad	Utilidad	439.321.833	4,39	1.256.740.204	12,57	1.837.064.604	18,37	11,78	CUMPLE
	Capital	100.000.000		100.000.000		100.000.000			
Capital Operativo	Activo corriente	1.135.721.499	649.999.040	2.156.604.488	1.353.827.419	3.529.245.223	2.670.508.949	330.118.579	CUMPLE
	Pasivo corriente	485.722.459		802.777.069		858.736.274			
									2.200.790.526

Empresa:		STARK TECNOLOGIA S.A.							
		2013		2014		2015		Promedio	Observaciones
Ratio de Liquidez	Activo corriente	5.473.127.628	1,67	8.961.160.758	1,33	7.365.116.487	81,73	28,24	CUMPLE
	Pasivo corriente	3.272.950.731		6.758.486.073		90.110.906			
Endeudamiento	Pasivo total	3.272.950.731	0,57	6.758.486.073	0,67	90.110.906	0,01	0,42	CUMPLE
	Activo total	5.696.067.850		10.078.625.249		8.318.353.199			
Rentabilidad	Utilidad	861.061.745	2,87	1.053.181.050	3,51	802.309.116	2,67	3,02	CUMPLE
	Capital	300.000.000		300.000.000		300.000.000			
Capital Operativo	Activo corriente	5.473.127.628	2.200.176.897	8.961.160.758	2.202.674.683	7.365.116.487	7.275.005.581	467.850.000	CUMPLE
	Pasivo corriente	3.272.950.731		6.758.486.073		90.110.906			
									3.119.000.000

Empresa:		ITC S.A.							
		2013		2014		2015		Promedio	Observaciones
Ratio de Liquidez	Activo corriente	1.912.693.780	5,13	3.432.545.978	2,13	4.224.534.248	1,99	3,09	CUMPLE
	Pasivo corriente	372.686.414		1.609.983.341		2.120.230.157			
Endeudamiento	Pasivo total	372.686.414	0,13	1.609.983.341	0,39	2.120.230.157	0,45	0,33	CUMPLE
	Activo total	2.794.987.703		4.105.859.718		4.894.896.676			
Rentabilidad	Utilidad	187.580.966	0,04	37.252.290	0,01	58.291.041	0,01	0,02	CUMPLE
	Capital	5.000.000.000		5.000.000.000		5.000.000.000			
Capital Operativo	Activo corriente	1.912.693.780	1.540.007.366	3.432.545.978	1.822.562.637	4.224.534.248	2.104.304.091	529.022.400	CUMPLE
	Pasivo corriente	372.686.414		1.609.983.341		2.120.230.157			
									3.526.816.000

Empresa:		LOGICALIS PARAGUAY S.A.							
		2013		2014		2015		Promedio	Observaciones
Ratio de Liquidez	Activo corriente	29.246.636.740	2,49	45.619.663.093	2,22	35.483.385.100	2,31	2,34	CUMPLE
	Pasivo corriente	11.740.223.341		20.525.913.880		15.378.396.999			
Endeudamiento	Pasivo total	11.740.223.341	0,39	20.525.913.880	0,45	15.378.396.999	0,43	0,42	CUMPLE
	Activo total	29.767.048.388		46.083.580.096		36.054.008.311			
Rentabilidad	Utilidad	5.805.239.183	52,77	7.506.275.860	68,24	10.345.213.823	94,05	71,89	CUMPLE
	Capital	110.000.000		110.000.000		110.000.000			
Capital Operativo	Activo corriente	29.246.636.740	17.506.415.399	45.619.663.093	25.093.749.213	35.483.385.100	20.104.988.101	630.000.000	CUMPLE
	Pasivo corriente	11.740.223.341		20.525.913.880		15.378.396.999			
									4.200.000.000

12. VERIFICACION DE LAS OFERTAS ECONOMICAS

Siguiendo el método de evaluación establecido en el **Art. 61 del Decreto 21.909/03 y el Decreto 5.174/05**, se ha procedido a la verificación aritmética de las ofertas presentadas por la firmas oferentes, en concordancia a lo estipulado en el Pliego de Bases y Condiciones, constatándose que las mismas **no poseen errores aritméticos**.-

13. ACLARACIONES LEGALES Y TÉCNICAS SOLICITADAS DURANTE EL PROCESO DE EVALUACIÓN.

En fecha 17 de agosto de 2017 vía correo electrónico, se solicita a la Coordinación de la Dirección Operativa de Contrataciones, el siguiente informe:
Informen si las personas citadas más abajo aparecen en la base de datos del SINARH o bien de la Secretaria de la Función Pública. Y si los mismos prestan servicios actualmente como funcionarios del Instituto de Previsión Social, en que área se desempeña.

LOGICALIS PARAGUAY:
ANTONIO ALFONSO DOMINGUEZ NOTARIO CI 885.593
ADRIANA PAVON KAM, CI 1188014
ALBERTO MOLLER PINGARILHO CI 94908994

Miguel Centurión
Dpto. de Tecnología
Dirección de Informática
Instituto de Previsión Social

STARK:
MARTIN MILCIADES NUÑEZ MARTINETTI, CI 1049058
LUCAS F BAEZ RAMIREZ CI 3786218

INSTITUTO DE PREVISION SOCIAL
Lic. Hermino Arturo Rivas
DIRECTOR DE EVALUACION

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Coronel Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

ITC:
ANGEL ALFREDO RAMON SEGOVIA, CI 1439760
ALBA MARIN DE SOSA, 4482504
MARIO ALBERTO BRUUN PAZ CI 1577463 (boliviano es representante del la señora alba marina sosa)

ONE:
FERNANDO A QUINTANA DA SILVA, CI 752135
OSCAR CARTES BARRIOCANAL, CI 1193544
MARIA ELENA NICORA DE PAATS, CI 611150
JUAN BAUTISTA CAZENAVE CARDUS, C.I. 457924
BLANCA PATRICIA GAYOSO SUGASTI C.I. 4154219

La Oficina de Coordinación remite el reporte el SINARH, según Memorándum N° 285/17 de fecha 17 de agosto de 2017, en el que se visualiza que las personas mencionadas no forman parte del plantel de funcionarios permanentes del Instituto de Previsión Social y de ningún organismo del Estado, por tanto no se encuentran comprendidos en las prohibiciones establecidas en el Art. 40, Inc. "a" y "b" de la Ley N° 2051/03.-

ONE S.A.
Se remitió la Nota N° 688/17 de fecha 14/08/2017 a la firma oferente, solicitando las siguientes documentaciones:

Estructura de Precio – Indicadores

- Costo de Producción: gastos por importación/arancel aduanero.
- Gastos Administrativos: salario del personal, carga social.
- Gastos de Distribución y/o Comercialización: flete, papelería.
- Otros Gastos
- Impuestos
- Ganancia

Respuesta: La firma presento lo solicitado, en tiempo y forma.

ONE S.A.
Se remitió la Nota N° 709/17 de fecha 17/08/2017 a la firma oferente, solicitando las siguientes documentaciones:

Sección VII – Anexos N° I Documentos que componen la Oferta
F. Cualquier otro documento adicional requerido
Punto 5. Deberá contar en su planilla de Aporte Obrero Patronal del mes anterior a la presentación de la oferta con 1 técnico certificado por el fabricante en la solución ofertada que será el responsable de la ejecución del proyecto. En caso de que el técnico certificado no sea parte del plantel permanente de la empresa oferente, se deberá presentar declaración jurada del mismo por la cual se compromete a firmar un contrato de trabajo para la ejecución del proyecto en caso de que la empresa oferente resulte adjudicada. Para la firma del Contrato se deberá presentar el Contrato de Trabajo, que debe extenderse por el tiempo requerido hasta culminar el proyecto, entre el técnico certificado propuesto en la oferta y la empresa adjudicada.
Respuesta: La firma presento lo solicitado, en tiempo y forma.

INFORMATICA TECNOLOGIA Y COMUNICACIÓN S.A. (ITC S.A.)
Se remitió la Nota N° 772/17 de fecha 23/08/2017 a la firma oferente, solicitando las siguientes documentaciones:

Sección VII – Anexos N° I Documentos que componen la Oferta
F. Cualquier otro documento adicional requerido

INSTITUTO DE PREVISION SOCIAL
Lic. Herminio Ramón Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

Miguel Centurión
Jefe de Departamento
Oficina de Informática
Instituto de Previsión Social

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Soroa Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicación

Punto 1. Presentar copias de Contratos y/o Facturas a través de las cuales el oferente demuestre haber facturado en la provisión de Soluciones de Gestión de Identidad y/o Software de Seguridad de Red a Instituciones Públicas o Privadas dentro de los últimos 5 (cinco) años (2011 – 2012 – 2013 – 2014-2015), y que el volumen de negocios en su totalidad sea igual o superior al 50% (cincuenta por ciento) del valor de su oferta. Serán aceptadas referencias de implementación de soluciones de gestión de fabricante y/o integrador de la solución ofertada.

Respuesta: La firma presento lo solicitado, en tiempo y forma.

14. RECOMENDACIÓN DE LA COMISION EVALUADORA:

En base a lo expuesto anteriormente y de acuerdo a las evaluaciones realizadas conforme al Art. 4 PRINCIPIOS GENERALES de la Ley 2051/03 y su Decreto Reglamentario, y Resoluciones DNCP N° 956/16 y 1173/16, vigentes desde el mes de abril del año 2016; El Comité de Evaluación de Ofertas eleva su Informe Final de Evaluación a la Dirección Operativa de Contrataciones y por su intermedio al Consejo de Administración con la siguiente sugerencia de **ADJUDICAR** a la firma **ONE S.A.**, la **LICITACIÓN PÚBLICA NACIONAL SBE N° 172/16 "ADQUISICIÓN DE SOFTWARE DE GESTION DE IDENTIDAD PARA EL IPS - AD REFERENDUM 2017"**, por cumplir con todos los requisitos legales y técnicos establecidos en el Pliego de Bases y condiciones, conforme al siguiente cuadro:

ONE S.A

ITEM	CODIGO DE CATÁLOGO	DESCRIPCIÓN DEL BIEN	UNIDAD DE MEDIDA	PRESENTACIÓN	CANTIDAD	MARCA	PROCEDENCIA	PRECIO UNITARIO C/IVA	PRECIO TOTAL C/IVA
1	43232402-003	Software de Gestion de Identidad	UNIDAD	UNIDAD	1	CA	USA	2.200.790.526	2.200.790.526
TOTAL GUARANIES DOS MIL DOSCIENTOS MILLONES SETECIENTOS NOVENTA MIL QUINIENTOS VEINTISEIS. (IVA INCLUIDO).-									**2.200.790.526**

MONTO TOTAL ADJUDICADO: (G. 2.200.790.526) SON GUARANÍES DOS MIL DOSCIENTOS MILLONES SETECIENTOS NOVENTA MIL QUINIENTOS VEINTISEIS (IVA INCLUIDO).

15. DOCUMENTOS REQUERIDOS PARA LA FIRMA DEL CONTRATO:

De conformidad a la evaluación realizada el oferente adjudicado deberá presentar para la suscripción del contrato los siguientes documentos:

- ✓ Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos.
- ✓ Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos.
- ✓ Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social.
- ✓ En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.

Es nuestro informe.

Miguel Centurión
Dpto. de Seguridad
Dirección de Informáticos
Instituto de Previsión Social

Miguel Darío Centurión Barreto
Dirección de Tecnología de la Información y las Comunicaciones

Abg. Leticia Pamela Giménez Mendiola
Dirección Jurídica

INSTITUTO DE PREVISION SOCIAL
Lic. Víctor Corvalan Giret
Oficina de Seguridad Informática
Dirección de Tecnología de la Información y Comunicaciones

Lic. Víctor Ramón Corvalan Giret
Dirección de Tecnología de la Información y las Comunicaciones

INSTITUTO DE PREVISION SOCIAL
Lic. Herminio Ramón Rivas
DIRECCION OPERATIVA DE CONTRATACIONES

Lic. Herminio Ramón Rivas
Dirección Operativa de Contrataciones