0000011

DIRECCIÓN DE TÉC. DE LA INFORMACIÓN Y COMUNICACIONES
INSTITUTO DE PREVISION SOCIAL
Fosento B
25 FEB 2020
RECIBIDO
9:20

INSTITUTO DE PREVISIÓN SOCIAL

■ TETÃ REKUÁI
■ GOBIERNO NACIONAL

Paraguay de la gente

DTIC/DTC/Nº16/2020

MEMORANDUM

PARA	: Dirección de Tecnología de la Información y Comunicaciones.
DE	: Departamento de Tecnología.
REFERENCIA	: **Solicitud de Inicio de llamado – Certificado Digital y Token de Seguridad**
LUGAR Y FECHA	: Asunción, 24 de febrero de 2020

MEM-0132-2020-000015

Me dirijo a Usted, y por su intermedio a la Dirección Operativa de Contrataciones, al objeto de solicitar el inicio de los trámites para el llamado a Licitación de Certificado Digital y Token de Seguridad para el IPS.

El objeto del llamado es generar condiciones que den mayor seguridad a ciertos procesos y con el uso de la Firma Digital garantizar la certeza de los datos consignados en los documentos. La implementación de la Firma Digital logrará que los procesos resulten más eficientes, ahorren papel, logren un mayor control, sean más flexibles y tengan un mayor alcance.

Por lo expuesto, solicito tenga a bien dar curso favorable a lo solicitado.

Se adjuntan los siguientes documentos:

- Formulario de Solicitud de Inicio de llamado.
- Especificaciones Técnicas.
- Formulario de PAC.
- Comparativos de Presupuestos.

Sin otro particular me despido de usted,

Atentamente,

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
Dirección de Tecnologías de la Información y de las Comunicaciones

INSTITUTO DE PREVISION SOCIAL
Dirección de Tecnología de la Información y Comunicaciones

☐ DAD	☐ DSU	☒ AT
☐ DTC	☐ DSIS	☐ OSI

OTRO
Obs.: A sus efectos
Fecha: 25/02/2020 Firma:

Gerencia de Abastecimiento y Logística
wjara

2020-12-10 12:22:18.421821

FORMULARIO DE SOLICITUD DE CONTRATACION

1	**FUNDAMENTACIÓN:**	Generar condiciones que den mayor seguridad a ciertos procesos y con el uso de la Firma Digital garantizar la certeza de los datos consignados en los documentos. La implementación de la Firma Digital logrará que los procesos resulten más eficientes, ahorren papel, logren un mayor control, sean más flexibles y tengan un mayor alcance.
2	**DESCRIPCIÓN:**	Adquisición de Certificados Digitales y Token de Seguridad para el IPS
3	**SISTEMA DE ADJUDICACIÓN**	Por el Total
4	**RUBROS Y PROGRAMAS A SER UTILIZADOS:**	Se indica en la Planilla de Precios
5	**SE UTILIZARÁ LA MODALIDAD CONTRATO ABIERTO**	Aplica. Se propone la modalidad de Contrato Abierto, porque durante la ejecución del Contrato se determinará la cantidad de procesos y por ende, de personas que utilizarán la firma digital y se pagará por los certificados y token que efectivamente sean necesarios una vez definidos los procesos a ser incluidos.
6	**AUTORIZACIÓN DEL FABRICANTE**	Aplica
7	**VISITA TÉCNICA**	No Aplica.
8	**MUESTRAS**	No Aplica.
9	**ESPECIFICACIONES TÉCNICAS**	Se Adjunta
10	**UNIDAD DE MEDIDA**	Unidad
11	**PRESENTACION**	Unidad
12	**PLAN DE ENTREGA:**	Se emitirán Órdenes de Entrega conforme a la necesidad del Administrador del Contrato, y en la misma se indicará la cantidad de certificados digitales y/o token que se requieran. **Ítem 1 - Certificado Digital:** Se debe coordinar con el Administrador del Contrato fecha y hora para el proceso de registro y emisión de certificado, y la misma deberá fijarse y ejecutarse dentro de los 5 días de recibida la Orden de Entrega por parte del proveedor. **Ítem 2 - Token de Seguridad**: Dentro de los 3 días posteriores a la recepción de la Orden de Entrega por parte del Proveedor.
13	**CONDICIONES DE PAGO**	Contra entrega con la presentación del Acta de Recepción Satisfactoria y /o Acta de Conformidad según corresponda.
14	**INSPECCIONES Y PRUEBAS:**	**Ítem 1 - Certificado Digital**: Consiste en la verificación del registro y emisión del certificado, y de ser satisfactoria se emitirá Acta de Conformidad en un plazo de 3 días hábiles a partir de la fecha del registro, de lo contrario se emitirá Nota de rechazo en el mismo plazo. **Ítem 2 - Token de Seguridad**: Se verificará que los token entregados correspondan a lo ofertado y cumplan con las prestaciones requeridas, así como su correcto funcionamiento. Se emitirá Acta de Recepción Satisfactoria en un plazo de 3 días hábiles a partir de la fecha de la Nota de Remisión, de lo contrario se emitirá Nota de rechazo en el mismo plazo.
15	**MULTAS:**	0,1% del valor del bien en demora por cada día de atraso
16	**PLAZO PARA REEMPLAZAR LOS BIENES:**	3 días contados a partir de la notificación del rechazo
17	**GARANTÍA TÉCNICA**	**Para el Ítem 1**: 24 meses **Para el Ítem 2**: 12 meses.
18	**VIGENCIA DEL CONTRATO**	26 meses contados desde la suscripción del contrato
19	**GARANTÍA DE FIEL CUMPLIMIENTO**	24 meses contados a partir de la firma del contrato
20	**ADMINISTRADOR DEL CONTRATO**	Dirección de Tecnología de la Información y de las Comunicaciones a través del Departamento de Tecnología
21	**DOCUMENTOS REQUERIDOS A LOS OFERENTES**	Resolución de Habilitación para operar como Prestador de Servicios de Certificación dentro de la infraestructura de Clave Pública de la República del Paraguay, emitida por el Ministerio de Industria y Comercio.
22	**PLANILLA DE PRECIOS ESTIMADOS**	Se Adjunta
23	**FIRMAS INVITADAS**	**DOCUMENTA** - RUC: 80050172-1 **VIT** - RUC: 80080099-0 **OPEN CODE** - Dirección: Aviadores del Chaco, 2050 World Trade Center Torre 3 - Piso 6 - Teléfono: 021 603 640 **DATA SYSTEMS** - RUC: 80013889-9 **PS LINE** - RUC 80028474-7

Gerencia de Abastecimiento y Logística
Vijaria

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
Dirección de Tecnologías de la Información y de las Comunicaciones

2020-12-10 12:22:18.421821

PROGRAMA ANUAL DE CONTRATACIONES
(Artículo 12° de la Ley N° 2.051/2003)

EJERCICIO FISCAL 2020

Nivel de Entidad:
Entidad:
UOC/UEP:
Sub UOC:
Unidad Jerarquica:
Código SICP:

Nro. PAC	MODALIDAD	FECHA ESTIMADA DEL LLAMADO	OBJETO DEL LLAMADO	MONEDA	PLURIANUALIDAD - (SI/NO)	PROVISORIO	MONTO TOTAL
	Contratación Directa	mar - 2020	Bienes	Guaraníes	Sí	NO	**24.282.000**

MONTOS POR EJERCICIO FISCAL

AÑO:	Objeto Gasto	2020	2021	2022	2023	2024	2025	2026	TOTAL
PROG 1	570	6.070.500	6.070.500	-	-	-	-	-	12.141.000
	340	6.070.500	6.070.500	-	-	-	-	-	12.141.000
									24.282.000

SBE	Inc. C) Decreto 5174/05	FONACIDE
SI/NO	SI/NO	SI/NO

CATEGORIA DEL BIEN/SERVICIO	DESCRIPCIÓN DEL PAC
24- Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento	Adquisición de Certificados Digitales y Token de Seguridad para el IPS

ITEM	CODIGO CATALOGO	DESCRIPCION DEL BIEN Y/O SERVICIO	PRECIO UNITARIO	MONTO MÍNIMO	MONTO MÁXIMO
1	43232402-002	Certificado Digital	404.700	12.141.000	24.282.000
2	43211711-9999	Token de Seguridad	404.700		

TIPO		PRG.	SUBP.	F.F.	O.F.	SGOG	F.F.	O.F	DPTO.	MONTO Gs.
		001				570				12.141.000
		001				340				12.141.000
									TOTAL:	**24.282.000**

Ley que rige el convenio (Solo en caso de ser proyecto): _____

FIRMA, SELLO
FUNCIONARIO RESPONSABLE DE LA U.O.C.

FIRMA, SELLO
MAXIMA AUTORIDAD DE LA INSTITUCION

fecha de elaboracion:

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
Dirección de Tecnologías de la Información
y de las Comunicaciones

Gerencia de Abastecimiento y Logística
Wjara

2020-12-10 12:22:18.421821

6003000

PRECIOS REFERENCIALES - Adquisición de Certificados Digitales y Token de Seguridad para el IPS

Código de Catálogo	ítem	Descripción	Empresa	Precio Unitario Gs	Promedio
43232402-002	1	Certificado Digital	Documenta S.A.	409400	404.700
			VIT S.A.	400000	

Código de Catálogo	ítem	Producto	Empresa	Precio Unitario Gs	Promedio
43211711-9999	1	Token	Documenta S.A.	409400	404.700
			VIT S.A.	400000	

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
Dirección de Tecnologías de la Informa
y de las Comunicaciones

Gerencia de Abastecimiento y Logística
wjara

Especificaciones Técnicas

Ítem 1 – Certificado Digital

DESCRIPCIÓN	ESPECIFICACIÓN TÉCNICA
1. Emisor	Los certificados deben ser emitidos por un prestador de servicios de certificación habilitado por el Ministerio de Industria y Comercio, y subordinado a la autoridad de certificación raíz del Paraguay.
2. Conformes al formato definido por la norma ITU X.509 o ISO/IEC 9594-8.	La estructura básica del certificado debe estar en conformidad a la norma que rige la materia y que la gramática utilizada tanto en la estructura básica como en las extensiones obligatorias, conforme a la norma ITU X.509 o ISO/IEC 9594-8
3. Tipo de certificado	Certificado de Persona Física del tipo F2 (Firma Digital basado en hardware)
4. Almacenamiento	La clave privada correspondiente al certificado digital debe ser generada en un dispositivo criptográfico (token) que asegure el cumplimiento del estándar FIPS 140 level 3
5. Duración	La validez del certificado digital deberá ser de 24 meses
6. Procedimiento de registro y emisión de certificado y par de claves	Presencial, en el local del Proveedor y/o en el local del IPS, cuya duración por proceso no supere 1 (una) hora.
7. Procedimiento de revocación de certificado	Presencial o remoto, el suscriptor debe poder revocar el certificado las 24 horas de los 7 días de la semana.
Estructura del certificado	
Campo Sujeto	
8. País	Código de país es asignado de acuerdo al estándar ISO 3166
9. Organización	En este campo se identifica el tipo de certificado. En este caso se identifica que corresponde a un certificado de persona física con datos laborales.
10. Unidad Organizativa	En este campo se indica el propósito del uso del certificado digital y el módulo (software/hardware) en el que fue almacenada la clave privada del titular del certificado. En este caso se identifica que corresponde a un certificado emitido en módulo hardware.
11. Nombres	Este campo debe contener el/los nombre/s y apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apóstrofes si corresponde.
12. Número de Serie	Debe contener las siglas CI seguidas del Número de Cédula de Identidad del titular del certificado, según documento de identificación.

Gerencia de Abastecimiento y Logística
Vijora

NSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
ión de Tecnologías de la Información
y de las Comunicaciones

2020-12-10 12:22:18.421821

13. Nombres	Este campo debe contener el/los nombre/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apóstrofes si corresponde.
14. Apellidos	Este campo debe contener el/los apellido/s del titular del certificado, según documento de identificación, en mayúsculas y sin tildes, a excepción de la Ñ. Podrán ser incluidos diéresis y apóstrofes si corresponde.
Campo Nombre Alternativo del Sujeto	
Rfc822Name	Email del titular del certificado.
15. Nombre de la Empresa	Nombre de la organización en el que presta servicio el titular del certificado.
16. Unidad Organizativa	Nombre de la unidad de la organización en el que presta servicio el titular del certificado.
17. Registro Único de Contribuyente	RUC más Número de cédula tributaria correspondiente a la organización en el que presta servicio el titular del certificado.
18. Cargo	Cargo del titular del certificado.
Campos relevantes	
19. Versión	V3
20. Número de Serie	Código identificador único del certificado dentro del ámbito del PSC
21. Algoritmo de Firma	El algoritmo de firma debe ser como mínimo sha256RSA encryption
22. Algoritmo hash de firma	sha256
23. Emisor	Identificación del Prestador de Servicios de Certificación (PSC), con indicación de su Razón Social, RUC, Código de país que se especifica en las directivas obligatorias para la formulación y elaboración de la Política de Certificación y Declaración de prácticas de certificación de los prestadores de servicios de certificación habilitados en la República del Paraguay.
24. Plazo de vigencia	Fecha de inicio y fecha de vencimiento
25. Clave pública del sujeto	Este campo indica la clave pública del titular del certificado. Codificado de acuerdo con el RFC 5280 y con un largo de clave de 2048 bits o 4096 bits y algoritmo RSA Encryption
26. Identificador de la Clave del Sujeto	Este campo debe contener el hash SHA-1 de la clave pública del titular del certificado. Este Campo es usado por el software de validación para ayudar a identificar un certificado que contiene una determinada clave pública. No es crítico.
27. Identificador de la clave de la entidad emisora	Debe contener el hash SHA-1 de la clave pública del PSC emisor del certificado. Este campo es usado por los diversos software de validación para ayudar a identificar a la autoridad certificadora que emitió el certificado en la cadena de Confianza. No es crítico.

Gerencia de Abastecimiento y Logística
wjara

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
Dirección de Tecnologías de la Información
y de las Comunicaciones
2020-12-10 12:22:18.421821

	En certificados tipo F2 solamente pueden ser activados los siguientes
28. Uso de la clave	bits: · NonRepudiation (renombrado recientemente con el nombre de contentCommitmen); · digitalSignature; · keyEncipherment Si es crítico
29. Uso extendido de la clave	Referencia otros propósitos de la clave, adicionales al uso y debe ser consistente con la extensión keyUsage. Si es crítico.
30. Pólizas de Certificado	Debe contener el OID de la CP correspondiente y la dirección WEB de la CPS del PSC que emite el certificado. No es crítico.
31. Restricciones Básicas	En este campo debe ir "TRUE" si el certificado corresponde a una CA o "FALSE" si no corresponde.
32. Nombre alternativo del sujeto	Campos no obligatorios. Rfc822Name= [email del titular del certificado]
33. CRLDistributionPoints	Este Campo es usado para indicar las direcciones donde puede ser encontrado el CRL correspondientes a la CA que emitió el certificado, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. No es crítico.
34. AuthorityInfoAcesss	Este Campo es usado para indicar las direcciones donde puede ser encontrado el certificado del PSC. Además, para indicar la dirección donde puede accederse al servicio de OCSP, de tal forma que se pueda validar si el certificado en cuestión ha sido revocado o no. La primera entrada debe contener el método de acceso id-ad-calssuer, utilizando uno de los siguientes protocolos de acceso: HTTPS o LDAP, para la recuperación de la cadena de certificación. La segunda entrada puede contener el método de acceso id-ad-ocsp con el respectivo respondedor OCSP utilizando uno de los siguientes protocolos de acceso HTTPS o LDAP. No es crítico.

Gerencia de Abastecimiento y Logística
Vijara

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
Dirección de Tecnologías de la Información
y de las Comunicaciones

Ítem 2 – Token de Seguridad

DESCRIPCIÓN	ESPECIFICACIÓN TÉCNICA
1. Sistemas operativos en los que opera (32 o 64 bits)	Windows XP SP3, Server2003 , Windows Vista, Server2008, Windows 7, Windows Server 2012, Windows 8, Windows 10
	Linux
	MAC OS X
2. Middleware	Microsoft Windows MiniDriver
	Windows middleware for Windows CSP
	Direct-called library for PKCS#11 under Windows, Linux and MAC
3. Standards	X.509 v3 Certificate Storage, SSL v3, IPSec, Minimamente ISO 7816 1-4 y opcionalmente ISO 7816 8 9 12, CCID
4. Algoritmos Criptográficos	RSA 2048 bit, como mínimo.
	SHA-1 / SHA-256
5. Longitud de Claves RSA	1024 bits/2048 bits
6. Funciones Criptográficas	Onboard key pair generation
	Onboard digital signature and verification
	Onboard data encryption and decryption
7. APIs Criptográficas	Microsoft Crypto API (CAPI), Cryptography API: Next Generation (CNG)
	Microsoft Smart Card MiniDriver
	PKCS#11
	IPSec/IKE
	PC/SC
8. Procesador	16 bit smart card chip (Common Criteria EAL 5+ certified). El procesador debe estar homologado por el Ministerio de Industria y Comercio (MIC)
9. Espacio de Memoria	Mínimamente: 64KB (EEPROM)
10. Dimensión	Mínimamente: 16,4mm*8,5mm*40,2mm
11. Reescritura de Celdas de Memoria	At least 500,000 write/erase cycles
12. Retención de Datos	Por lo menos 10 años
13. Certificaciones de Seguridad	FIPS 140-2 level 3
14. Interface de Comunicación	USB 1.1 y 2.0 full speed & high speed, Connector type A
15. Interface	ISO 7816
	CCID
16. Consumo de Energía	Less than 250mW. Máximo 5 V.
17. Temperatura de Funcionamiento	0°C ~ 70°C
	(32°F ~ 158°F)

Gerencia de Abastecimiento y Logística
Wjara

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
ción de Tecnologías de la Información
y de las Comunicaciones

2020-12-10 12:22:18.421821

18. Temperatura de Almacenamiento	-20°C ~ 85°C (-4°F ~ 185°F)
19. Humedad	0% ~ 100% sin condensación
20. Compatibilidad con especificaciones de la Organización Internacional de Normalización (ISO)	Compatible con las especificaciones 1 a 4 de la Norma ISO/IEC 7816
21. Resistencia al Agua	IPX7/IPX8, with glue injection (under evaluation)

INSTITUTO DE PREVISION SOCIAL
Francisco Santacruz
Jefe, Dpto. de Tecnología
Dirección de Tecnologías de la Información
y de las Comunicaciones

Gerencia de Abastecimiento y Logística
Wjara

VIT S.A.
España 2028 casi Brasilia
Teléfono: 595-21- 229-350 / 207-732 / 207-733
(0981) 957-554 / (0981) 955-439
www.efirma.com.py

Asunción, 17 de febrero de 2020.-

PROPUESTA COMERCIAL

Señores: IPS
Atención: Lic. Giselle Echeverria
Presente:

Tenemos el agrado de presentarles la propuesta comercial para la adquisición de Certificados Digitales. La emisión de Certificados digitales eFirma se realiza en módulos de almacenamiento seguro y homologado.

Certificados digitales para Personas Físicas con Datos Laborales

PERSONA FÍSICA	Precio Unitario IVA Incluido Gs
Certificado Digital Con válidez de 2 años	400.000
Token de Seguridad	400.000
Servicio de RA Móvil. El servicio de RA MÓVIL: es un servicio en el cual los funcionarios de eFirma se trasladan a sus instalaciones para realizar el proceso de emisión y entrega del certificado digital. ***OBS: Este ítem debe ser considerado en el llamado teniendo en cuenta que en las especificaciones técnicas se solicita entrega en el local de IPS.***	600.000

Los Precios están expresados en Guaraníes, IVA Incluido.

Sin otro particular nos despedimos muy cordialmente.

RAQUEL FABIOLA VILLALBA CACERES
Firmado digitalmente por RAQUEL FABIOLA VILLALBA CACERES
Fecha: 2020.02.17 11:01:22 -03'00'

VIT S.A. - eFirma

Gerencia de Abastecimiento y Logística
Wijara

2020-12-10 12:22:18.421821

Gisselle Echeverria Galeano

De: Javier Davalos <jdavalos@documenta.com.py>
Enviado el: lunes, 17 de febrero de 2020 15:32
Para: Gisselle Echeverria Galeano
CC: Francisco Santacruz
Asunto: Re: solicitud de presupuesto - Certificado digital y Token de Seguridad

Buenas tardes Lic. Gisselle;

A continuación la cotización por certificados digitales y Token de Seguridad generados en oficinas de Documenta SA. Todos los precios sin IVA incluido.

- Ítem 1: Certificado Digital: 409.400 Gs.
- Ítem 2: Token de Seguridad: 409.400 Gs.

Tomando en cuenta que en las EE.TT. se establece que las emisiones podrían realizarse en oficinas de IPS a través del sub-ítem 6 *"Procedimiento de registro y emisión de certificado y par de claves: Presencial, en el local del Proveedor* ***y/o en el local del IPS****, cuya duración por proceso no supere 1 (una) hora.",* estaríamos necesitando que se agregue la cantidad de emisiones o la posibilidad de cotizar el servicio de generación en oficinas externas a las del oferente. Actualmente este servicio se cotiza aparte y el monto alcanza los 600.000 Gs. IVA incluido por evento.

Cualquier consulta, a las órdenes.

Saludos cordiales

documenta

Javier Dávalos
Jefe Operaciones y Producto
0981 184141
jdavalos@documenta.com.py
Avda. Rca. Argentina Nro. 893
casi Alberto de Souza, Asunción-Paraguay
(595 021 492501/3 • 0800 113365
www.digito.com.py

DIGITO

El 14/2/2020 a las 10:13, Gisselle Echeverria Galeano escribió:

> Buenos días Sres. Documenta,
>
> En virtud del inicio de los trámites para el llamado de la Licitación de Adquisición de Certificado Digital y Token de Seguridad, le solicito tenga a bien remitir por este medio un presupuesto ajustado a las EE.TT. adjuntas, de manera a proseguir con los tramites de rigor.
>
> En espera de un despacho favorable, le saludo,
>
> Atte.

Lic. Gisselle Echeverria
Departamento de Tecnología
Dirección de Tecnologías de la Información y Comunicaciones
Email: gechever@ips.gov.py IP: 10151– Tel: 021.219.7100

TETÃ REKUÁI
GOBIERNO NACION
Paraguay de la gente

3er. Piso - Edif. Caja Central - Constitución y Herrera

Gerencia de Abastecimiento y Logística
Wjara

2020-12-10 12:22:18.421821