SECRETARÍA DE INNOVACION PÚBLICA
SUBSECRETARÍA DE GESTIÓN ADMINISTRATIVA DE INNOVACIÓN PÚBLICA
DIRECCIÓN DE GESTIÓN PROGRAMAS Y PROYECTOS

PROYECTO DE MODERNIZACIÓN E INNOVACIÓN PARA MEJORES SERVICIOS PÚBLICOS EN ARGENTINA - PMISP

PRÉSTAMO Nº: 8710-AR

DOCUMENTO DE LICITACIÓN

Adquisición de Renovación Integral de la Infraestructura de Firma Digital de la Autoridad Certificante- Oficina Nacional de Tecnologías de la Información

CODIGO STEP:

AR-SIP-177262-NC-RFB

SDO 03/2020

BANCO INTERNACIONAL DE RECONSTRUCCIÓN Y FOMENTO

Fecha de Apertura

XX de XXXX de XXXX a las XX horas.

LLAMADO A LICITACIÓN

Proyecto: Proyecto de Modernización e Innovación para Mejores Servicios Públicos en Argentina - PMISP

Préstamo Nº: 8710-AR

Solicitud de Oferta N° 03/2020

Adquisición de:

Renovación Integral de la Infraestructura de Firma Digital de la Autoridad Certificante- Oficina Nacional de Tecnologías de la Información

1. La República Argentina ha recibido un préstamo del Banco Internacional de Reconstrucción y Fomento para financiar parcialmente el costo del ***Proyecto de Modernización e Innovación para Mejores Servicios Públicos en Argentina***, ***Préstamo BIRF 8710-AR.*** Se propone utilizar parte de los fondos de tal préstamo para efectuar los pagos del Contrato Solicitud de Ofertas N° ***03/2020-CODIGO STEP: AR-SIP-177262-NC-RFB***, para la "***Adquisición de Renovación Integral de la Infraestructura de Firma Digital de la Autoridad Certificante-Oficina Nacional de Tecnologías de la Información".***

La Dirección de Gestión, Programas y Proyectos de la Subsecretaría de Gestión Administrativa de Innovación Pública de la Secretaría de Innovación Pública invita a los licitantes elegibles a presentar ofertas selladas para la "***Adquisición de Renovación Integral de la Infraestructura de Firma Digital de la Autoridad Certificante- Oficina Nacional de Tecnologías de la Información"***, de acuerdo al siguiente detalle:

LOTE	ITEM	CANTIDAD
LOTE UNICO	**1.1.Equipamiento** **1.1.2 Switches de Red** **1.1.3 Servidores de Red Genéricos** **1.1.4 Firewall**	 **4 (cuatro)** **10 (diez)** **8 (ocho)**
	1.2.Actualización funcional de la Plataforma para nuevas prestaciones	**1 (uno)**
	1.3 Migración de la Plataforma actualizada a la nueva infraestructura	**1 (uno)**
SERVICIOS CONEXOS	**1.4 Capacitación/cursos**	**4 (cuatro)**
	1.5 Soporte Técnico integral	**ANUAL**

2. Los licitantes elegibles que estén interesados podrán obtener información adicional de la Dirección de Gestión Programas y Proyectos, enviando un correo electrónico a **dgpyp@jefatura.gob.ar**

3. Los requisitos de calificación incluyen Experiencia y capacidad Técnica, de acuerdo a lo especificado en la Cláusula 3.9.1 del Pliego.

4. Los licitantes interesados podrán obtener un juego completo de los Documentos de Licitación, enviando un correo electrónico a la siguiente dirección: **dgpyp@jefatura.gob.ar**

5. Las ofertas deberán presentarse a través del portal COMPR.AR, a más tardar, a las **xxxx horas del xx de xxxx de xxxx**. Las ofertas que se reciban fuera

de plazo serán rechazadas.

6. Todas las ofertas deberán estar acompañadas de un “Manifiesto de Garantía de la Oferta”.

INDICE

6. **Recepción de los bienes y servicios y plazo de garantía**
7. **Solución de Controversias**
8. **Prórroga de jurisdicción**
9. **Penalidades**

E. ESPECIFICACIONES TÉCNICAS

Anexo 1: FORMULARIO DE LA OFERTA

Anexo 2: LISTA DE PRECIOS

Anexo 3: SERVICIOS CONEXOS

Anexo 4: MANIFIESTO DE GARANTÍA DE LA OFERTA

Anexo 5: LISTA DE BIENES Y SERVICIOS Y PLAN DE ENTREGAS

Anexo 6: AUTORIZACIÓN DEL FABRICANTE

Anexo 7: MODELO DE CONTRATO

Anexo 8: GARANTÍA DE CONTRATO

A.

A. ASPECTOS GENERALES

1.1 Fuente de Recursos

1.1.1 La República Argentina ha recibido del Banco Internacional de Reconstrucción y Fomento (BIRF) un préstamo para financiar parcialmente el costo del **Proyecto de Modernización e Innovación para Mejores Servicios Públicos en Argentina- Préstamo BIRF 8710-AR**. En tal contexto, podrán participar en la licitación todos los interesados de los países que reúnan los requisitos de elegibilidad que se estipulan en las *Regulaciones de Adquisiciones para Prestatarios en Proyectos de Inversión del Banco Mundial.*

1.2 Terminología

1.2.1 Las expresiones que aquí se definen se aplican al presente documento y a sus formularios y planillas adjuntas:

(a) **Receptora - Prestatario**: es la República Argentina.

(b) **B.I.R.F o Banco**: es el Banco Internacional de Reconstrucción y Fomento (BIRF).

(c) **Préstamo**: es el Convenio de Préstamo 8710-AR celebrado entre el B.I.R.F. y el Prestatario.

(d) **Proyecto**: es el ***Proyecto de Modernización e Innovación para Mejores Servicios Públicos en Argentina***

(e) **Comprador**: Dirección de Gestión Programas y Proyectos, que se encarga de la adquisición de los bienes y servicios, la cual figura designada como tal en las Bases y Condiciones que integran la documentación de esta Solicitud de Oferta.

(f) **Proveedor**: es la persona de existencia ideal o visible que ha formalizado el Contrato y se encuentra obligada al suministro de los bienes y servicios, en los términos previstos.

(g) **Días**: son días calendario y meses son meses calendario. salvo disposición en contrario.

1.3 Marco legal

1.3.1 Durante la adquisición, el Proyecto está obligado a regirse por las normas del Convenio de Préstamo, las Regulaciones de Adquisiciones del BIRF y las estipulaciones del presente documento. Cuando exista vacío normativo o deba resolverse sobre aspectos no reglamentados en este Documento

de Licitación, se aplicarán supletoriamente las normas que de acuerdo a derecho correspondan a la jurisdicción del Contratante y a la personería de éste, siempre que no se opongan a lo establecido en: i) el Convenio de Préstamo y ii) las Regulaciones de Adquisiciones para Prestatarios en Proyectos de Inversión del BIRF.

1.3.2 En todos los casos y cualquiera sea la personería del Contratante, se entenderá que el Contrato que se celebre con el adjudicatario de la licitación es un Contrato de provisión de bienes y servicios regido por la ley de la República Argentina.

1.4 Corrupción o Prácticas Fraudulentas

1.4.1 El Banco exige que todos los Prestatarios (incluidos los beneficiarios de préstamos concedidos por el Banco), así como los Licitantes, proveedores, contratistas y sus agentes (hayan sido declarados o no), el personal, los subcontratistas, proveedores de servicios o proveedores de insumos que participen en proyectos financiados por el Banco, observen las más estrictas normas de ética durante el proceso de licitación y de ejecución de dichos contratos[1]. Para dar cumplimiento a esta política, el Banco:

(a) define, a los efectos de esta disposición, las siguientes expresiones:

i. por "práctica corrupta" se entiende el ofrecimiento, entrega, aceptación o solicitud directa o indirecta de cualquier cosa de valor con el fin de influir indebidamente en el accionar de otra parte;
ii. por "práctica fraudulenta" se entiende cualquier acto u omisión, incluida la tergiversación de información, con el que se engañe o se intente engañar en forma deliberada o descuidadamente a una parte con el fin de obtener un beneficio financiero o de otra índole, o para evadir una obligación;
iii. por "práctica colusoria" se entiende todo arreglo entre dos o más partes realizado con la intención de alcanzar un propósito ilícito, como el de influir de forma indebida en el accionar de otra parte;
iv. por "práctica coercitiva" se entiende el perjuicio o daño o la amenaza de causar perjuicio o daño directa o indirectamente a cualquiera de las partes o a sus bienes para influir de forma indebida en su accionar;
v. por "práctica obstructiva" se entiende:

a) la destrucción, falsificación, alteración u ocultamiento deliberado de pruebas materiales referidas a una investigación o el acto de dar falsos testimonios a los investigadores para impedir materialmente que el

[1] Las inspecciones que se llevan a cabo en este contexto suelen ser de carácter investigativo (es decir, forense). Consisten en actividades de constatación realizadas por el Banco o por personas nombradas por éste para abordar asuntos específicos relativos a las investigaciones/auditorías, como determinar la veracidad de una denuncia de fraude y corrupción a través de los mecanismos adecuados. Dicha actividad incluye, entre otras cosas, acceder a la información y los registros financieros de una empresa o persona, examinarlos y hacer las copias que corresponda; acceder a cualquier otro tipo de documentos, datos o información (ya sea en formato impreso o electrónico) que se considere pertinente para la investigación/auditoría, examinarlos y hacer las copias que corresponda; entrevistar al personal y otras personas; realizar inspecciones físicas y visitas al emplazamiento y someter la información a la verificación de terceros.

Banco investigue denuncias de prácticas corruptas, fraudulentas, coercitivas o colusorias, o la amenaza, persecución o intimidación de otra parte para evitar que revele lo que conoce sobre asuntos relacionados con una investigación o lleve a cabo la investigación, o

b) los actos destinados a impedir materialmente que el Banco ejerza sus derechos de inspección y auditoría establecidos en el párrafo 1.4 e. que figura a continuación.

(b) Rechazará toda propuesta de adjudicación si determina que la empresa o persona recomendada para la adjudicación, los miembros de su personal, sus agentes, subconsultores, subcontratistas, prestadores de servicios, proveedores o empleados han participado, directa o indirectamente, en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas para competir por el contrato en cuestión.

(c) Además de utilizar los recursos legales establecidos en el convenio legal pertinente, podrá adoptar otras medidas adecuadas, entre ellas, declarar que las adquisiciones están viciadas, si determina en cualquier momento que los representantes del Prestatario o de un receptor de una parte de los fondos del préstamo participaron en prácticas corruptas, fraudulentas, colusorias, coercitivas u obstructivas durante el proceso de adquisición, o la selección o ejecución del contrato en cuestión, y que el Prestatario no tomó medidas oportunas y adecuadas, satisfactorias para el Banco, para abordar dichas prácticas cuando estas ocurrieron, como informar en tiempo y forma a este último al tomar conocimiento de los hechos.

(d) Sancionará, conforme a lo establecido en sus directrices de lucha contra la corrupción y a sus políticas y procedimientos de sanciones vigentes incluidas en el Marco de Sanciones del Grupo Banco Mundial, a cualquier empresa o persona que, según determine en cualquier momento, haya participado en actos de fraude y corrupción en relación con el proceso de adquisición, la selección o la ejecución de los contratos que financie.

(e) Exigirá que en los documentos de SDO/SDP y en los contratos financiados con préstamos del Banco se incluya una cláusula en la que se exija que los licitantes (postulantes/proponentes), consultores, contratistas y proveedores, así como sus subcontratistas, subconsultores, agentes, empleados, consultores, prestadores o proveedores de servicios, permitan al Banco inspeccionar[2] todas las cuentas, registros y otros documentos referidos al proceso de adquisición y la selección o la ejecución del contrato, y someterlos a la auditoría de profesionales nombrados por este.

[2] Un subcontratista, consultor, fabricante y/o un proveedor de productos o servicios (se usan diferentes nombres según el documento de licitación utilizado) nominado es aquel que ha sido: (i) incluido por el licitante en su aplicación u oferta de precalificación por cuanto aporta la experiencia clave y específica y el conocimiento que permite al licitante cumplir con los criterios de calificación para un proceso de precalificación o licitación en particular; o (ii) nominado por el prestatario.

1.5 Requisitos para los Licitantes

1.5.1 Un Licitante y todas las partes que constituyen el Licitante, pueden tener la nacionalidad de cualquier país, de conformidad con las condiciones estipuladas en la Sección C, Elegibilidad. Se considerará que un Licitante tiene la nacionalidad de un país si es ciudadano o está constituido, incorporado o registrado y opera de conformidad con las disposiciones legales de ese país. Este criterio también aplicará para determinar la nacionalidad de los subcontratistas o proveedores propuestos para la ejecución de cualquier parte del Contrato, incluso los Servicios Conexos.

1.5.2 Un Licitante no deberá tener conflicto de interés. Si se considera que algún licitante posee conflicto de interés, será descalificado. Se considerará que los Licitantes tienen conflicto de interés con una o más partes en este proceso de licitación si ellos:

(a) están o han estado asociados, directa o indirectamente, con una firma, o con cualquiera de sus afiliados, que ha sido contratada por el Comprador para la prestación de servicios de consultoría para la preparación del diseño, las especificaciones técnicas y otros documentos que se utilizarán en la licitación para la adquisición de los bienes y servicios objeto de estos Documentos de Licitación;

(b) o presentan más de una oferta en este proceso licitatorio.

1.5.3 Una firma que haya sido inhabilitada por el Banco de acuerdo a lo establecido en la Subclausula 1.4.1 (d) de la Sección A, o de acuerdo con las Normas para la Prevención y Lucha contra el Fraude y la Corrupción en proyectos financiados por préstamos del BIRF y donaciones de la (AIF) estará inhabilitada para la adjudicación de contratos financiados por el Banco y/o recibir cualquier beneficio de un contrato financiado por el Banco, financiero o de otra índole, durante el periodo determinado por el Banco. La lista de firmas inhabilitadas se encuentra disponible en la dirección electrónica que se indica a continuación: http://www.worldbank.org/debarr.

1.5.4 Las empresas estatales del país Prestatario serán elegibles solamente si pueden demostrar que (i) tienen autonomía legal y financiera; (ii) operan conforme a las leyes comerciales; y (iii) no dependen de ninguna agencia del Comprador.

1.5.5 Los Licitantes deberán proporcionar al Comprador evidencia satisfactoria de su continua elegibilidad, cuando el Comprador razonablemente la solicite.

B. INSTRUCCIONES A LOS LICITANTES

2. Solicitud de Oferta

2.1 Domicilio y Notificaciones

2.1.1. El domicilio y correo electrónico consignado y debidamente actualizado en el portal COMPR.AR, serán los constituidos para el presente procedimiento. Las notificaciones que en los mismos se efectúen se considerarán válidas, fehacientes y notificadas el mismo día en el que fueron enviadas, siendo suficiente la constancia que tales medios generen. Asimismo, se considerarán cumplidas, a sus efectos, todas las notificaciones que se efectúen y/o publiquen automáticamente mediante la plataforma COMPR.AR.

2.1.2 Todas las notificaciones entre la jurisdicción o entidad contratante y los interesados, oferentes, adjudicatarios o cocontratantes se realizarán válidamente a través de la difusión en el sitio de internet del portal COMPR.AR, cuya dirección es https://comprar.gob.ar o la que en un futuro la reemplace y se entenderán realizadas el día hábil siguiente al de su difusión.
El envío de mensajería mediante la plataforma COMPR.AR en forma automática, solo constituye un medio de aviso.
Se recomienda a los interesados revisar periódicamente el portal COMPR.AR – en particular el Escritorio del Proveedor- para informarse de las novedades vinculadas a las etapas, desarrollo del proceso de contratación electrónica y demás información relevante.
La no recepción oportuna de correos electrónicos de alerta que envía el COMPR.AR, no justificará, ni se considerará como causal suficiente para eximir a los proponentes de sus cargas y responsabilidades."

2.2. Características del procedimiento

2.2.1 Todo posible licitante que requiera alguna aclaración sobre los Documentos de Licitación deberá comunicarse con el Comprador mediante correo electrónico a: **dgpyp@jefatura.gob.ar** El Comprador responderá por escrito a todas las solicitudes de aclaración, siempre que dichas solicitudes sean recibidas al menos siete (7) días antes de la fecha límite para la presentación de ofertas, es decir, hasta el día xx de xxxx de xxxx. El Comprador enviará simultáneamente copia de las respuestas, incluyendo una descripción de las consultas realizadas, sin identificar su fuente, a todos los destinatarios de los documentos originales y a todos los posibles licitantes que figuren en los registros. Si como resultado de las aclaraciones, el Comprador considera necesario enmendar los Documentos de Licitación, deberá hacerlo siguiendo el procedimiento indicado en la Subcláusula 2.2.2.

2.2.2 El Comprador podrá, en cualquier momento antes del vencimiento del plazo para presentación de ofertas, enmendar los Documentos de Licitación mediante la emisión de una enmienda. Toda enmienda emitida formará parte integrante de los Documentos de la Licitación y deberá ser publicada en los mismos medios donde se publicó el Documento de Licitación.

2.3 Cotización y contratación

2.3.1 El licitante cotizará la totalidad de los ítems y el 100% de las cantidades solicitadas para cada ítem por el que se compromete a proveer los bienes y servicios solicitados y detallados de acuerdo a las Especificaciones Técnicas requeridas. La cotización y contratación se hará en pesos argentinos. Con

respecto al Item 1.1., al ser bienes importados, se podrá realizar la cotización en dólares estadounidenses. Sin embargo, aún en este último supuesto el pago se realizará en pesos argentinos de acuerdo al tipo de cambio estipulado en la cláusula 4.6 del presente. En el Formulario de la Oferta deberá consignarse el precio total de la oferta.

3. Ofertas

3.1 Presentación de las ofertas

3.1.1 Solo se aceptarán las ofertas que se presenten a través del portal COMPR.AR, hasta el día y hora que determine el comprador en la convocatoria, utilizando el formulario electrónico que suministre el sistema, cumpliendo todos los requerimientos de los pliegos aplicables y acompañando la documentación que la integre en soporte electrónico. A fin de garantizar su validez, la oferta electrónicamente cargada deberá ser confirmada por el oferente, quien podrá realizarlo únicamente a través de un administrador legitimado para ello, conforme lo normado con el procedimiento de registración y autenticación de los usuarios de los proveedores. Sólo aquella oferta CONFIRMADA quedará registrada en el acto de apertura de ofertas. La edición de una oferta sin confirmación posterior a la apertura equivale al retiro de la misma.
En ningún caso el licitante podrá alegar el mal funcionamiento o errores del sitio de Internet de la plataforma COMPR.AR para eximirse o aducir excepciones respecto del ingreso oportuno de cualquier dato, información o documentación requerida en los formularios electrónicos habilitados, estando aquél obligado a guardar la debida diligencia y antelación para ingresar y confirmar su oferta en el portal COMPR.AR en los plazos perentorios establecidos en el presente documento.

3.1.2 Las ofertas tendrán una **validez de noventa (90) días** a partir de la fecha de su apertura y los documentos que las integran deberán presentarse firmados por el Licitante en todas sus fojas.

3.1.3 En circunstancias excepcionales y antes de que expire el período de validez de la oferta, el Comprador podrá solicitarle a los Licitantes que extiendan el período de la validez de sus ofertas. Las solicitudes y las respuestas deberán hacerse por escrito. Al Licitante que acepte la solicitud de prórroga no se le pedirá ni permitirá modificar su oferta. En caso de silencio por parte del Licitante, implicará la negativa a la extensión del plazo del período de validez de oferta.

3.2 Manifiesto de Garantía de la Oferta

3.2.1 Todas las ofertas deberán incluir un Manifiesto de Garantía de la Oferta, usando el modelo indicado en el Anexo 4 de estos documentos.

3.2.2 El Manifiesto de Garantía de la Oferta de una Asociación en Participación o Consorcio deberá ser emitido en nombre de la Asociación en Participación o Consorcio que presenta la oferta. Si dicha Asociación o Consorcio no ha

sido legalmente constituido en el momento de presentar la oferta, el Manifiesto de Seriedad de la Oferta deberá ser emitido en nombre de todos los futuros socios de la Asociación o Consorcio y firmada por cada miembro.

3.3 Documentos que integran la oferta

3.3.1 La oferta deberá incluir los siguientes documentos:

(a) Formulario de la Oferta (Anexo 1);
(b) Lista de cantidades y precios de cada renglón (Anexo 2)
(c) Formulario de Servicios Conexos –en caso de corresponder- (Anexo 3);
(d) Especificaciones técnicas de los bienes y servicios ofertados, no se admitirá la especificación "según Pliego" como identificación del servicio o equipamiento ofrecido, pudiéndose adjuntar folletos y/o catálogos ilustrativos en idioma castellano y fotografías de los ítems cotizados como complementarios de la oferta presentada, como así también ampliación de las especificaciones técnicas o cualquier otro elemento informativo de interés que permita una mejor evaluación de los elementos cotizados.
(e) Copia de la documentación que acredite la constitución de la persona jurídica conforme a las normas que rijan la creación de dichas instituciones.
(f) Copia del poder (escritura pública) en que se otorguen facultades al firmante de la oferta para comprometer al licitante;
(g) Copia del formulario de inscripción en el ente tributario.
(h) Manifiesto de Garantía de la Oferta (Anexo 4).
(i) En el caso de manifestar compromiso formal de conformar una asociación en participación, consorcio o asociación (en adelante Consorcio) la siguiente documentación certificada por escribano público:

i.1) Poder emitido por las personas que conformarán el Consorcio o sus representantes legales en favor de uno de ellos, mediante el cual se acrediten sus facultades para suscribir la oferta y actuar en su representación desde el momento de la presentación de la propuesta hasta el dictado del acto de finalización del procedimiento.

i.2. Declaración jurada suscripta por las personas que conformarán el Consorcio o sus representantes legales, en la que conste lo siguiente:

i.2.1. El compromiso de constituirse legalmente como tal, en caso de resultar adjudicatarias, y de modo previo a la suscripción del contrato respectivo.

i.2.2. El compromiso expreso de responsabilidad principal, solidaria e ilimitada de todas y cada una de las personas agrupadas, por el cumplimiento de todas las obligaciones emergentes del procedimiento de selección y del contrato.

i.2.3. El compromiso de mantener la vigencia del Consorcio por un plazo no menor al fijado para el cumplimiento de todas las obligaciones emergentes del contrato.

i.2.4. El compromiso de no introducir modificaciones en el estatuto del

Consorcio, ni en el de las personas jurídicas que la integraren, que importe una alteración de la responsabilidad, sin la aprobación previa del Comprador.

i.2.5. El compromiso de actuar exclusivamente bajo la representación unificada en todos los aspectos concernientes al contrato.

i.3. Documentación que acredite el cumplimiento de los requisitos específicos previstos en el Pliego los que deben ser cumplidos en conjunto por todos ellos.

Una vez presentada la oferta, el Consorcio no podrá modificar su integración, es decir, cambiar, aumentar y/o disminuir el número de personas que las compondrán, y en caso de ser contratadas no podrán hacerlo hasta el cumplimiento total de las obligaciones emergentes del contrato, excepto conformidad expresa del Comprador.i.1) Acreditación de la constitución y representación legal de cada una de las empresas que lo conforman (contrato social y sus modificaciones, con constancia de su inscripción en el Registro Público respectivo).

i.2) Carta de Intención de conformar el consorcio debidamente firmada por los representantes legales de cada una de las empresas que lo integrarán, con indicación de la firma que actuará como principal.

Cada una de las empresas integrantes de una asociación en participación, consorcio o asociación deberá cumplir con los requisitos exigidos en los puntos e) y f).

(j) Asimismo, deberá presentar toda la documentación exigida en la **Cláusula 3.8.1. a) Adjudicación de Contrato, para acreditar lo solicitado**.

3.4 Formularios de oferta

3.4.1 El Licitante llenará el formulario de oferta incluido como Anexo 1, la lista de precios que se incluye en el Anexo 2 de estos documentos de licitación y el formulario de servicios conexos, si corresponde, indicado en el Anexo 3 e indicará la cantidad, los precios, y una breve descripción de los mismos. Asimismo, el Licitante deberá completar el Manifiesto de Garantía de la Oferta, indicado en el Anexo 4 y la Autorización del Fabricante/Distribuidor para el caso de los Bienes (Anexo 6)

3.5 Retiro, sustitución o modificación de oferta

3.5.1. Un Licitante podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por mail, de conformidad con la Subcláusula 3.1.1, debidamente firmada por un representante autorizado. Asimismo, deberá incluir una copia de tal autorización (poder notarial). La sustitución o modificación de la oferta deberá acompañar dicha comunicación por escrito. Todas las comunicaciones deberán ser recibidas por el Comprador antes del plazo límite establecido para la presentación de las ofertas, de conformidad con la Subcláusula 3.1.1. Los sobres deberán estar claramente marcados bajo el rótulo "RETIRO", "SUSTITUCIÓN" o "MODIFICACIÓN".

Las ofertas cuyo retiro fue solicitado de conformidad con la presente Subcláusula serán devueltas sin abrir a los Licitantes remitentes.

Ninguna oferta podrá ser retirada, sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado por el Licitante en el Formulario de Oferta, o cualquier extensión si la hubiese.

3.6. Apertura de las ofertas

3.6.1. La apertura de ofertas se efectuará por acto público a través del portal COMPR.AR. En forma electrónica y automática se generará el acta de apertura de ofertas correspondiente.

3.7. Análisis y evaluación de las ofertas

3.7.1. La información relativa al examen, aclaración, evaluación y comparación de las ofertas y las recomendaciones para la adjudicación de un contrato no podrán ser reveladas a los licitantes ni a ninguna otra persona que no participe oficialmente en dicho proceso hasta que se haya notificado la intención de adjudicación del contrato.

3.7.2. El Comprador examinará las ofertas para determinar si están completas, si contienen errores de cálculo, si se han presentado las garantías requeridas y si los documentos han sido debidamente firmados. En caso de errores aritméticos procederá a corregirlos de la siguiente manera:

(a) si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido a menos que el Comprador considere que hay un error obvio en la colocación del punto decimal, caso en el cual el total cotizado prevalecerá y el precio unitario se corregirá;

(b) si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total; y

(c) si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (a) y (b) mencionados. En caso de discrepancia de precios establecidos en la planilla de cotización generada por la plataforma COMPR.AR y cualquier otra planilla de cotización que el licitante también pudiera presentar, se tomará como válida la detallada en la primera de las citadas planillas.

Si el Licitante que presentó la oferta evaluada más baja no acepta la corrección de los errores, su oferta podrá ser rechazada y se podrá ejecutar el Manifiesto de Garantía de la Oferta.

3.7.3 El Comprador examinará todas las ofertas para confirmar que todos los documentos y documentación técnica solicitada en la Subcláusula 3.3.1 de

la Sección B han sido suministrados y para determinar si cada documento entregado está completo.

3.7.4 El Comprador confirmará que los siguientes documentos e información han sido proporcionados con la oferta. Si cualquiera de estos documentos o información faltaran, la oferta será rechazada y, por lo tanto no será evaluada.

(a) Formulario de Oferta firmado, de conformidad con el formulario del Anexo 1;

(b) Lista de Precios firmada, de conformidad con el formulario del Anexo 2;

(c) Formulario de Servicios Conexos firmado, si corresponde, de conformidad con el formulario del Anexo 3;

(d) Manifiesto de Garantía de la Oferta firmado, de conformidad con el formulario del Anexo 4.

En la evaluación de las ofertas el Comprador tendrá en cuenta, además del precio ofrecido, los costos de transporte y seguro y el cumplimiento de las especificaciones técnicas ó características básicas de los bienes y servicios.

Las ofertas que no se ajusten al período de validez indicado en la Subcláusula 3.1.2 de la Sección B, serán rechazadas.

3.7.5 El Comprador evaluará y comparará las ofertas que se ajusten a los requisitos de los documentos de licitación.

3.7.6 La evaluación se hará por Lote Único. Pero deberán cotizar por el 100% de los bienes y servicios que conformar el lote y por el 100% de las cantidades solicitadas para el lote.

3.7.7 Los oferentes deberán presentar una única oferta en la que se incluyan las provisiones de bienes y los servicios requeridos en el presente pliego para el lote único y los servicios conexos; todo ello, de conformidad con las Especificaciones Técnicas – Punto E.

3.8 Derecho del Comprador a Aceptar Cualquier Oferta y a Rechazar Cualquiera o Todas las Ofertas

3.8.1 El Comprador se reserva el derecho a aceptar o rechazar cualquier oferta, de revocar el proceso licitatorio y de rechazar todas las ofertas en cualquier momento antes de la adjudicación del Contrato, sin que por ello genere responsabilidad alguna ante los Licitantes.

3.9 Requisitos de Poscalificación

3.9.1 El Contratante adjudicará el Contrato al Licitante cuya Oferta se ajuste a

las condiciones y requisitos de estos Documentos y resulte ser la de precio evaluado más bajo, siempre y cuando reúnan los requisitos de poscalificación especificados en el Llamado a Licitación y en esta cláusula.

Los requisitos de calificación incluyen:

a) **Experiencia y capacidad técnica**

El Licitante deberá proporcionar prueba documental que demuestre que cumple los siguientes requisitos de experiencia y capacidad técnica:

1. Haber ejecutado en los últimos diez (10) años al menos cuatro (4) proyectos en soluciones informáticas en el ámbito de la Administración Pública Nacional o Provincial, de los cuales dos (2) deben ser de gestión integral de infraestructura de Firma Digital. A estos efectos acompañará a su propuesta el detalle de:

   - ✓ Cliente (Denominación, Dirección)
   - ✓ Contacto Técnico (Nombre y teléfono)
   - ✓ Breve descripción de los trabajos ejecutados
   - ✓ Fecha de inicio y finalización

2. El licitante deberá cumplir con los siguientes requisitos y competencias comprobadas en Argentina y presentar documentación que lo acredite:

- ❖ Contar con un contrato de soporte Microsoft Premier Support Services. Se deberá adjuntar nota de Microsoft certificando la disponibilidad del mismo o copia del contrato vigente.

3. El licitante deberá haber satisfecho los requisitos y ser parte del programa de Microsoft Partner Network con al menos siguientes competencias:

- ❖ Gold Desarrollo de aplicaciones
- ❖ Gold Datacenter

4. El licitante deberá presentar documentación que acredite que todos los recursos pertenezcan a su planta permanente de personal, y deberá acompañar los CV de los consultores y documentación respaldatoria al momento de formular su oferta.
5. El licitante deberá presentar la autorización del fabricante/distribuidor de cada uno de los productos ofertados, por la cual se lo autoriza a distribuir y comercializar sus productos. Esta exigencia no será aplicable en el caso de aquellos productos cuyos fabricantes no posean sede oficial en nuestro país.

3.9.2 En caso de presentarse un Consorcio o Asociación de Empresas, la oferta se evaluará en forma conjunta sumando las calificaciones de cada firma.

La información para cada una de las firmas asociadas deberá sumarse para determinar el cumplimiento del Licitante con los criterios mínimos requeridos; sin embargo, para que una firma asociada califique, el socio responsable deberá satisfacer, por lo menos, el cuarenta por ciento (40 %) de esos criterios mínimos estipulados como criterios para un Licitante individual y los otros socios, al menos, el veinticinco por ciento (25%) de estos criterios. El incumplimiento de este requisito podrá dar como resultado el rechazo de la asociación. La experiencia y recursos de los subcontratistas no se tomarán en cuenta para determinar el cumplimiento del Licitante con los criterios establecidos como requisitos.

3.9.3 El Comprador se reserva el derecho, al momento de adjudicar el contrato, de incrementar o reducir las cantidades de los servicios especificados en los documentos de licitación, siempre y cuando esta variación no exceda el veinte por ciento (20%) del total de los servicios sin conformidad del Proveedor y hasta un treinta y cinco por ciento (35%) con conformidad del Proveedor, no podrá modificar los precios unitarios y los términos y condiciones de los documentos de licitación y de la Oferta.

3.10 Plazo Suspensivo

3.10.1 El Contrato no se adjudicará antes de la finalización del Plazo Suspensivo. El Plazo de Suspensión será de tres (3) días hábiles. El Plazo Suspensivo comenzará el día posterior a la fecha en que el Comprador haya transmitido a cada Licitante la Notificación de Intención de Adjudicación del Contrato. Cuando solo se presente una Oferta, o si este contrato es en respuesta a una situación de emergencia reconocida por el Banco, no se aplicará el Plazo Suspensivo.

3.11 Notificación de Intención de Adjudicación

3.11.1 La notificación de la intención de adjudicar se realizará a todos los oferentes mediante la difusión en el sitio https://comprar.gob.ar o en el que en un futuro lo reemplace y se enviarán avisos mediante mensajería del COMPR.AR.

3.11.2 El Comprador transmitirá a todos los Licitantes la Notificación de Intención de Adjudicar el Contrato al Licitante seleccionado. La Notificación deberá contener, como mínimo, la siguiente información:

- ✓ el nombre y la dirección del Licitante que presentó la Oferta seleccionada;
- ✓ el precio del Contrato de la Oferta seleccionada;
- ✓ los nombres de todos los Licitantes que presentaron Ofertas y los precios de sus Ofertas, tal como se leyeron en voz alta en la apertura de las Ofertas;
- ✓ una declaración donde se expongan las razones por las cuales no fue seleccionada la Oferta del Licitante no seleccionado a quien se notifica,
- ✓ la fecha de vencimiento del Plazo Suspensivo; y
- ✓ instrucciones sobre cómo solicitar explicaciones y/o presentar una queja durante el Plazo Suspensivo.

Los Licitantes no favorecidos tendrán un plazo de tres (3) días hábiles para presentar una solicitud de explicaciones por escrito dirigida al Comprador. El Comprador deberá brindar las explicaciones correspondientes a todos los Licitantes cuya solicitud se reciba dentro del plazo establecido.

3.12 Adjudicación

3.12.1 Antes del vencimiento del Período de Validez de la Oferta y del vencimiento del Plazo Suspensivo, según se especifica en la cláusula 3.10, o de cualquier prórroga otorgada, si la hubiera, y tras la resolución satisfactoria de cualquier queja que se haya presentado en el curso del Plazo Suspensivo, se notificará la adjudicación a todos los que participaron del procedimiento, mediante la difusión en el sitio https://comprar.gob.ar o en el que en un futuro lo reemplace y se enviarán avisos mediante mensajería del COMPR.AR.

3.12.2 La adjudicación recaerá en un solo oferente y será por la totalidad del lote.

3.13 Firma del Contrato

3.13.1 La notificación del respectivo contrato al adjudicatario se realizará mediante la difusión en el sitio https://comprar.gob.ar o en el que en un futuro lo reemplace y se enviarán avisos mediante mensajería del COMPR.AR.
El contrato quedará perfeccionado desde la suscripción del mismo. El Proveedor tendrá un plazo de 10 (diez) días desde la notificación hacerlo efectivo.

Cuando el Licitante seleccionado presente la garantía de cumplimiento de conformidad con el Formulario del Anexo 8 y suscriba el contrato, el Comprador publicará el aviso de adjudicación de contrato.

3.14 Garantía de cumplimiento de Contrato

3.14.1 El adjudicatario deberá integrar la garantía de cumplimiento del contrato equivalente al DIEZ POR CIENTO (10 %) del monto total de la adjudicación, de conformidad con el Anexo 8, dentro del plazo de CINCO (5) días de notificada la suscripción del contrato. La garantía deberá ser ingresada a través del COMPR.AR, utilizando el formulario electrónico que suministre el sistema a tales efectos.

3.14.2 Se podrá ejecutar la garantía de cumplimiento por ceder el contrato sin autorización de la jurisdicción o entidad contratante

3.14.3 La Garantía de Cumplimento será liberada por el Comprador y devuelta al Proveedor a más tardar a los treinta (30) días contados a partir de la fecha de recepción definitiva de los bienes y servicios.

3.15 Asociación en Participación o Consorcio

Si el Proveedor es una Asociación en Participación o Consorcio, todas las partes que lo conforman serán mancomunada y solidariamente responsables frente al Comprador por el cumplimiento de las disposiciones del Contrato

y designarán a una de ellas para que actúe como representante con autoridad para comprometer a la Asociación en Participación o Consorcio. La composición o constitución de la Asociación en Participación o Consorcio no podrá ser alterada sin el previo consentimiento del Comprador.

3.16 Ordenes de Cambio y Enmiendas al Contrato

3.16.1 El Comprador podrá, en cualquier momento, efectuar cambios dentro del marco general del Contrato, mediante orden escrita al Proveedor.
Si cualquiera de estos cambios causara un aumento o disminución en el costo o en el tiempo necesario para que el Proveedor cumpla cualquiera de las obligaciones en virtud del Contrato, se efectuará un ajuste equitativo al Precio del Contrato o al Plan de Entregas/de Cumplimiento, o en ambas cuestiones, y el Contrato se enmendará según corresponda. El Proveedor deberá presentar la solicitud de ajuste de conformidad con esta Cláusula, dentro de los veintiocho (28) días contados a partir de la fecha en que éste reciba la solicitud de la orden de cambio del Comprador.

Los precios que cobrará el Proveedor por Servicios Conexos que pudieran ser necesarios pero que no fueron incluidos en el Contrato, deberán convenirse previamente entre las partes, y no excederán los precios que el Proveedor cobra actualmente a terceros por servicios similares.

Sujeto a lo anterior, no se introducirá ningún cambio o modificación al Contrato excepto mediante una enmienda por escrito ejecutada por ambas partes.

C. ELEGIBILIDAD

Elegibilidad para el suministro de bienes, la contratación de obras y prestación de servicios en adquisiciones financiadas por el Banco

1. De acuerdo con el párrafo 3.21 de las Regulaciones de Adquisiciones para Prestatarios en Proyectos de Inversión, publicadas por el Banco en julio de 2016 y revisadas en noviembre de 2017 y agosto de 2018, el Banco le permite a firmas e individuos de todos los países suministrar bienes, obras y servicios para proyectos financiados por el Banco. Excepcionalmente, las firmas de un país o los bienes fabricados en un país podrían ser excluidos si:

a. Las empresas o los individuos de un país o los Bienes fabricados en un país podrán considerarse inadmisibles en los siguientes casos:

i. Si como consecuencia de leyes o normas oficiales, el país del Prestatario prohíbe las relaciones comerciales con ese país, siempre que el Banco considere que dicha exclusión no impide la competencia efectiva en el suministro de los Bienes, las Obras o los Servicios de No-Consultoría, ni en la contratación de los Servicios de Consultoría. Cuando el proceso de adquisición traspase fronteras jurisdiccionales (cuando más de un país participe en dicho proceso), la exclusión de una empresa o de un individuo por estas razones puede aplicarse también en las adquisiciones que se realicen en los otros países participantes, siempre que el Banco y todos los Prestatarios involucrados en dichas adquisiciones estén de acuerdo.

ii. Cuando, en cumplimiento de una decisión del Consejo de Seguridad de las Naciones Unidas adoptada en virtud del Capítulo VII de la Carta de dicho organismo, el país del Prestatario prohíba la importación de Bienes de un país en particular o los pagos a un país, a una persona o entidad. Cuando el país del Prestatario prohíba los pagos a una empresa en particular o los pagos por Bienes específicos en virtud de un acto de cumplimiento de este tipo, se podrá excluir a dicha empresa.

b. Las instituciones o empresas de propiedad estatal del país del Prestatario podrán competir por un contrato y resultar adjudicatarias únicamente si demuestran, de un modo aceptable para el Banco, que:

i. son legal y financieramente autónomas;
ii. realizan operaciones de acuerdo con el derecho comercial;
iii. no están sometidas a la supervisión de la entidad que las contrata.

c. Quedarán excluidas las empresas o los individuos declarados inelegibles, sancionados conforme a las Normas para la Prevención y Lucha contra el Fraude y la Corrupción y de acuerdo con las políticas y procedimientos de sanciones vigentes incluidos en el Marco de Sanciones del Grupo Banco Mundial.

D. CONDICIONES DEL CONTRATO

4.1 Inicio y Plazo de ejecución

Los bienes y servicios objeto del presente llamado deberán prestarse de acuerdo con el Cronograma de Entregas y de Cumplimiento indicado en el Anexo 5. Los mismos deberán iniciarse dentro de los 10 días corridos contados a partir de la suscripción del contrato.

4.2 Confidencialidad-Derechos de Propiedad Intelectual

Toda la información proporcionada para la ejecución de las tareas que son encomendadas al contratante con motivo del presente es de exclusiva propiedad del Prestatario.
El proveedor y el personal que se encuentren ligados a la provisión de los servicios objetos del presente llamado están obligados a mantener la más estricta confidencialidad sobre la información que obtenga del Sector Público Nacional y/o la SECRETARÍA DE INNOVACIÓN PÚBLICA, en relación con el objeto del contrato. En tal sentido, los sujetos referidos en el párrafo que antecede no podrán comunicar a persona alguna la información sobre la que hayan tenido conocimiento con motivo de la ejecución de sus obligaciones emanadas del presente, salvo autorización expresa por parte de la SECRETARÍA DE INNOVACIÓN PÚBLICA. Esta obligación no se extinguirá con el cumplimiento del objeto del contrato.
La información, ideas, conceptos, práctica y/o técnicas a cuyo conocimiento el cocontratante acceda y/o se generen con motivo del contrato resultante del presente, forman parte del secreto institucional propiedad del Prestatario, por lo que el proveedor se compromete a: I) Mantener absoluta reserva de las mismas; II) Custodiarlas apropiadamente; III) No divulgarlas, ni transmitirlas a terceros no autorizados; IV) No explotarlas ni utilizarlas en beneficio propio y/o de terceros, salvo cesión y/o consentimiento previo y por escrito otorgado por la SECRETARÍA DE INNOVACIÓN PÚBLICA; V) En caso de que las tareas sean efectuadas por personal dependiente del cocontratante, este se compromete (con anterioridad al inicio de su trabajo) a poner en su conocimiento las presentes condiciones, asumiendo el proveedor la responsabilidad frente al incumplimiento de las mismas por su personal.
El incumplimiento de las obligaciones establecidas en los párrafos que anteceden será considerado falta gravísima y dará lugar a la rescisión del contrato por culpa del proveedor, sin perjuicio de las restantes penalidades y sanciones que pudieren corresponder.
El presente compromiso es irrevocable y seguirá siendo válido aún después de finalizada la relación con el Prestatario.
El proveedor se obliga a que la totalidad de los derechos de cualquier naturaleza o clase, derivados del presente contrato serán de propiedad exclusiva de la SECRETARÍA DE INOVACIÓN PÚBLICA, sin limitación espacial, territorial o temporal alguna.

Los derechos de propiedad intelectual, así como todo otro derecho de cualquier naturaleza, sobre los trabajos realizados, documentación, resultados de estudios y/o análisis, y cualquier otro producto derivado del cumplimiento del presente contrato, pertenecerán exclusivamente a la SECRETARÍA DE INNOVACIÓN PÚBLICA.

El proveedor deberá realizar o acordar la realización de cada acto, documento, etc. que la SECRETARÍA DE INNVACIÓN PÚBLICA pueda considerar necesario o deseable para perfeccionar el derecho, título y/o interés sobre dichos derechos.

En consecuencia, los datos, los documentos electrónicos que los contengan y, en general, las bases de datos, son de propiedad exclusiva de la SECRETARÍA DE INNOVACIÓN PÚBLICA y no podrán ser utilizados en actividades distintas de la de ejecución del contrato a que de origen este llamado.

Al término del contrato la información de las bases de datos antes referidas no podrá ser utilizada ni explotada en ninguna forma por el cocontratante, consultores y/o personal dependiente del mismo.

También se debe considerar como datos a la información propiamente dicha, más la documentación que indique como están estructurados los mismos, estructuras de integridad y relación. En caso de ser necesario su desarrollo, también se considerarán como datos, la documentación de los algoritmos y cálculos usados en la generación de los datos existentes en las bases de datos, documentación completa referida al análisis, diseño e implementación.

4.3 Dependencia Laboral

4.3.1 Todo el personal afectado a este servicio estará bajo exclusivo cargo del proveedor, corriendo por su cuenta salarios, seguros, leyes sociales y previsionales y cualquier otra erogación sin excepción, no teniendo en ningún caso, el mismo, relación de dependencia con la Administración Pública Nacional.

4.3.2. Por otra parte, queda entendido que la Administración Pública Nacional no asumirá responsabilidad alguna y estará desligado de todo conflicto o litigio que eventualmente se genere por cuestiones de índole laboral entre el proveedor y el personal que éste ocupara para prestar el servicio que se le ha contratado. Cada trabajador deberá ser notificado de esta situación y suscribir una declaración jurada de estilo, destacando al personal que la única relación laboral existente es la que lo vincula con el adjudicatario.

4.4 Contabilidad, inspección y auditoria por el Banco de los archivos del proveedor.

4.4.1 El Proveedor permitirá al Banco y/o a otras personas designadas por el Banco a inspeccionar los servicios, y/o las cuentas y registros del Proveedor y de sus sub-proveedores relativos a la Oferta del Proveedor y la ejecución del contrato, y tener tales cuentas y registros auditados por auditores designados por el Banco, si el Banco así lo exigiera. El Proveedor deberá tener presente lo previsto en la Subcláusula 5.1.1 (b) de las Condiciones del Contrato la cual prevé que todo acto dirigido a impedir de forma material el derecho del Banco a inspeccionar y auditar

establecido en la presente Subcláusula constituye una práctica prohibida sujeta a sanción por el Banco.

4.5 Inspección y Prueba de los bienes y servicios

Previo a la aceptación y recepción definitiva de los bienes y servicios detallados en el presente pliego de Especificaciones Técnicas, el área requirente del organismo procederá a comprobar que se han cumplido sin errores todos los procesos enumerados y solicitados en el detalle de bienes y servicios y en los ANEXOS de las Especificaciones Técnicas.

Esto es, una vez que el proveedor informe que ha concluido una etapa, el área requirente iniciará el proceso de verificación de los referidos procesos, generando un informe de todos los errores encontrados que se deben resolver.

Dicho informe será notificado al proveedor, el cual deberá resolver la lista de errores informados, dando prioridad a los marcados como críticos, para luego el área requirente volver a verificar todos los procesos.

Este ciclo de revisión continuará hasta que sean resueltos todos los errores marcados como críticos por parte del área requirente del organismo, durante un plazo máximo de 20 días corridos por etapa, luego del cual se comenzarán a aplicar penalidades abajo detalladas.

El retraso en el cumplimiento del plazo máximo para resolver todos los errores críticos indicados en las pruebas y comprobaciones a verificar para la recepción definitiva de cada etapa, dará lugar a que el contratante pueda imponer una penalización equivalente al CERO COMA CINCO POR CIENTO (0,5%) del presente contrato por cada día de retraso, deducible del pago de la factura correspondiente al desarrollo de las mismas.

El soporte técnico debe prestarse siempre que sea necesario y deberá contar con la conformidad del contratante con la misma periodicidad hasta la finalización del contrato. Por lo tanto, en los casos de incumplimientos de los plazos máximos de resolución que puedan motivar la imposición de la penalidad mencionada en el párrafo anterior, el proveedor deberá depositar en la cuenta bancaria que disponga el contratante la misma suma estipulada porcentualmente por cada día de penalización.

4.6 Pago

4.6.1 El pago de los bienes y servicios se realizará de la siguiente manera, de acuerdo a los plazos de entrega previstos a continuación:

1.1) Equipamiento:

1.1.a) El ciento por ciento (100 %) del monto correspondiente a este Item, se abonará contra entrega de la totalidad de los bienes que componen dicho ítem dentro del plazo de treinta (30) días de la firma del contrato, con la emisión de un certificado recepción definitiva por parte del Área Requirente del organismo.
En caso de que se hubiere cotizado en dólares estadounidenses dicho

importe se convertirá a pesos argentinos de acuerdo al tipo de cambio del Banco Nación de Argentina (BNA) Vendedor Billete correspondiente al día anterior al pago.

1.2) Actualización funcional de la Plataforma para nuevas prestaciones:

1.2.a) El diez por ciento (10%) del monto correspondiente a este ítem se abonará dentro de los 10 días de la firma del contrato contra entrega del "Plan de ejecución" (diagrama y criterios de validación de tareas), Dicho Plan deberá ser aprobado por el contratante.
1.2.b) El cuarenta por ciento (40%) del monto correspondiente a este ítem se abonará dentro de los 60 días de la firma del contrato contra entrega del "Diagrama de Base de Datos y Arquitectura" (front end, roles, capas servicios WFC, lógicas y validaciones para los desarrollos "Certificados de Aplicaciones", "Generación de Sitios Seguros" e "Integración RENAPER"); y Documento "Diseño Funcional de la solución" aprobados por el contratante.
1.2.c) El cincuenta por ciento (50%) restante del monto correspondiente a este ítem se abonará dentro de los 120 días de la firma del contrato contra entrega del "Ambiente de prueba de los desarrollos instalados en servidores del contratante; Informe "Prueba Funcional, reporte de fallas y soluciones de backlog" aprobados por el contratante, y código fuente y documentación final entregados.

1.3) Migración de la Plataforma:

1.3.a) El cincuenta por ciento (50%) del monto correspondiente a este ítem se abonará dentro de los 150 días de la firma del contrato contra entrega del "Esquema sobre instalación, configuración e interconexión realizada en hardware, networking y servidores", aprobada por el contratante.

1.3.b) El cincuenta por ciento (50%) restante del monto correspondiente a este ítem se abonará dentro de los 210 días de la firma del contrato contra entrega del Informe sobre arquitectura y políticas aplicadas realizadas en infraestructura Microsoft, de backup, de monitoreo y de migración de Infraestructura PKI al nuevo entorno operativo.

1.4) Capacitación:

1.4.a) El ciento por ciento (100 %) del monto correspondiente a este Item, se abonará dentro de los 240 días de la firma del contrato contra entrega de un "Informe de conformidad de cuatro cursos realizados" (detallando diseño de contenidos, fechas, lugares, docentes, asistentes y extensión) y conformidad del Contratante.

1.5) Soporte técnico integral

1.5.a) El ciento por ciento (100%) del importe correspondiente al Soporte Técnico anual se abonará dentro de los 30 días de comenzada la prestación,

una vez puesta en funcionamiento la solución en forma integral. Previo al pago deberá presentar una Póliza de Caución o garantía bancaria por el mismo importe, en garantía. Se abonará con la conformidad del Área requirente del organismo siempre que el servicio se brindó de acuerdo a lo establecido en el primer mes de vigencia, con el detalle de las actividades realizadas (tipo de incidente, fecha, hora, personal, resolución final).

4.6.2. Condiciones de Pago

Todos los pagos se efectuarán en pesos argentinos (AR$). El medio de pago a utilizar es la transferencia bancaria directa a la cuenta que indique el Proveedor o, en caso de requerirlo, un cheque.

Todos los pagos se efectuarán dentro de los treinta (30) días siguientes a la presentación de una solicitud de pago acompañada de un certificado del Comprador que indique que los servicios han sido recibidos y que todos los demás servicios contratados han sido cumplidos de conformidad.

4.6.3 Documentación de pago:

i. Original y copia de la Factura del Proveedor, en la que se describa al Comprador como ***Secretaría de Innovación Pública–CUIT 30-71511756-4*** y se indique en el detalle el número de Contrato de Préstamo BIRF 8710-AR, el nombre y número de la Licitación, y la descripción, cantidad, precio unitario y monto total de los equipos o trabajos realizados.
ii. Certificado de aceptación de conformidad emitido por el Área Requirente del organismo, para la percepción del pago.

5. Rescisión del contrato

5.1 Rescisión por causa del Proveedor

5.1.1 El Comprador tendrá derecho a rescindir el Contrato cuando el Proveedor:

a. Obre con dolo, culpa grave o reiterada negligencia en el cumplimiento de sus obligaciones.
b. Cuando incurra en alguna situación de caso fortuito o fuerza mayor debidamente documentada, de tal gravedad que coloquen al proveedor en una situación de razonable imposibilidad de cumplimiento de sus obligaciones.
c. A juicio del Comprador haya empleado prácticas corruptas, fraudulentas, colusivas, coercitivas u obstructivas al competir por ó en la ejecución del Contrato.

Para propósitos de esta cláusula:

i. "práctica corrupta" significa el ofrecimiento, suministro, aceptación o solicitud, directa o indirectamente, de cualquier cosa de valor con el fin de influir impropiamente en la

actuación de otra persona[3];

ii. "práctica fraudulenta" significa cualquier actuación u omisión, incluyendo una tergiversación de los hechos que, astuta o descuidadamente, desorienta o intenta desorientar a otra persona con el fin de obtener un beneficio financiero o de otra índole, o para evitar una obligación[4];

iii. "práctica de colusión" significa un arreglo de dos o más personas[5] diseñado para lograr un propósito impropio, incluyendo influenciar impropiamente las acciones de otra persona;

iv. "práctica coercitiva" significa el daño o amenazas para dañar, directa o indirectamente, a cualquiera persona, o las propiedades de una persona, para influenciar impropiamente sus actuaciones[6].

v. "práctica de obstrucción" significa

(aa) la destrucción, falsificación, alteración o escondimiento deliberados de evidencia material relativa a una investigación o brindar testimonios falsos a los investigadores para impedir materialmente una investigación por parte del Banco, de alegaciones de prácticas corruptas, fraudulentas, coercitivas o de colusión; y/o la amenaza, persecución o intimidación de cualquier persona para evitar que pueda revelar lo que conoce sobre asuntos relevantes a la investigación o lleve a cabo la investigación, o

(bb) las actuaciones dirigidas a impedir materialmente el ejercicio de los derechos del Banco a inspeccionar y auditar de conformidad con la Subcláusula 1.4.1 de la Sección A.

d. Si éste se declarase en quiebra o en estado de insolvencia. En tal caso, la terminación será sin indemnización alguna para el Proveedor, siempre que dicha terminación no perjudique o afecte algún derecho de acción o recurso que tenga o pudiera llegar a tener posteriormente hacia el Comprador.

5.2 Revocación por Oportunidad, mérito o Conveniencia

[3] "Persona" se refiere a un funcionario público que actúa con relación al proceso de contratación o la ejecución del contrato. En este contexto, "funcionario público" incluye a personal del Banco Mundial y a empleados de otras organizaciones que toman o revisan decisiones relativas a los contratos.

[4] "Persona" significa un funcionario público; los términos "beneficio" y "obligación" se refieren al proceso de contratación o a la ejecución del contrato; y el término "actuación u omisión" debe estar dirigida a influenciar el proceso de contratación o la ejecución de un contrato.

[5] "Personas" se refiere a los participantes en el proceso de contratación (incluyendo a funcionarios públicos) que intentan establecer precios de oferta a niveles artificiales y no competitivos.

[6] Persona" se refiere a un participante en el proceso de contratación o en la ejecución de un contrato.

5.2.1 El Comprador, mediante comunicación enviada al Proveedor, podrá revocar el Contrato total o parcialmente, en cualquier momento por razones de oportunidad, mérito o conveniencia. La comunicación de terminación deberá indicar que es por conveniencia del Comprador, el alcance de la terminación de las responsabilidades del Proveedor en virtud del Contrato y la fecha de efectividad de dicha terminación.

6. Recepción de los bienes y servicios y plazo de garantía

6.1 Una vez recibidos de conformidad, se labrará un Acta de Recepción de los bienes y servicios. Asimismo, el personal técnico del Comprador emitirá un certificado de aceptación que permitirá que el Proveedor presente la factura correspondiente. A partir de esta instancia, comenzará a regir la garantía establecida en las Especificaciones Técnicas.

7. Solución de Controversias

7.1 El Comprador y el Proveedor harán todo lo posible para resolver amigablemente mediante negociaciones directas informales, cualquier desacuerdo o controversia que se haya suscitado en virtud o en referencia al Contrato.

8. Prórroga de jurisdicción

8.1 Se deja establecido que cualquier contienda que surja de la contratación propiciada y no resuelta de acuerdo al procedimiento establecido en la cláusula anterior, así como también sobre la interpretación de cláusulas contractuales y/o del presente documento, serán dirimidas en los Tribunales en lo Contencioso Administrativo Federal con asiento en la Ciudad Autónoma de Buenos Aires. En consecuencia, quién resulte adjudicatario deberá constituir domicilio legal en la Ciudad Autónoma de Buenos Aires, donde se tendrán por válidas todas las notificaciones judiciales o extrajudiciales que deban practicarse.

9. Penalidades:

9.1. Los oferentes, adjudicatarios y cocontratantes serán pasibles de penalidades, cuando incurran en las siguientes causales:

a) Pérdida de la garantía de cumplimiento del contrato:

1.- Por incumplimiento contractual, si el cocontratante desistiere en forma expresa del contrato antes de vencido el plazo fijado para su cumplimiento, o vencido el plazo de cumplimiento original del contrato o de su extensión, o vencido el plazo de las intimaciones que realizara la Comisión de Recepción, en todos los casos, sin que los bienes fueran entregados o prestados los servicios de conformidad.

2.- Por ceder el contrato sin autorización de la jurisdicción o entidad contratante**.**

b) Multas durante la prestación del servicio

Para situaciones que el área requirente del organismo identifique como de criticidad alta, y en las que no se pueda dar una solución inmediata al problema, el contratista se compromete a realizar los mejores esfuerzos técnicos y profesionales que tiene a su disposición, a fin de encontrar una solución alternativa o temporal, hasta tanto se implemente la solución definitiva del problema.

En el caso que el proveedor no cumpla con los tiempos máximos establecidos anteriormente en lo referente a la disponibilidad, se procederá a ejecutar un descuento de las horas insumidas en el presente mes proporcional al perjuicio ocasionado.

Para todos los incidentes se establece que, una vez transcurrido el **tiempo de respuesta máximo**, por cada UNA (1) hora de retraso en responder la orden de pedido deberá depositar el DOS POR CIENTO (2%) del monto correspondiente al mes en curso hasta un máximo de DIEZ POR CIENTO (10%) por incidente, siendo acumulativos los descuentos que se hayan imputado debido al atraso en la atención de otros incidentes del mismo mes.

Se establece, además, penalidades por exceder el tiempo máximo de resolución según la criticidad del incidente:

a) **Criticidad Alta**: Una vez transcurrido el **tiempo de reparación máximo** para este tipo de incidentes, por cada UNA (1) hora de retraso en solucionar el incidente el proveedor deberá depositar en la cuenta indicada por el Contratante un valor equivalente al DOS POR CIENTO (2%) del monto mensual que correspondería al servicio de soporte hasta un máximo de DIEZ POR CIENTO (10%) por incidente, siendo acumulativos los importes que se hayan imputado debido al atraso en la reparación de otros incidentes del mismo mes.

b) **Criticidad Media**: Una vez transcurrido el **tiempo de reparación máximo** para este tipo de incidentes, por cada UNA (1) hora de retraso en solucionar el incidente proveedor deberá depositar en la cuenta indicada por el Contratante un valor equivalente al UNO POR CIENTO (1%) del monto mensual que correspondería al servicio de soporte hasta un máximo de DIEZ POR CIENTO (10%) por incidente, siendo acumulativos los importes que se hayan imputado debido al atraso en la reparación de otros incidentes del mismo mes.

c) **Criticidad Baja**: Una vez transcurrido el **tiempo de reparación máximo** para este tipo de incidentes, por cada UN (1) día de retraso en solucionar el incidente el proveedor deberá depositar en la cuenta indicada por el Contratante un valor equivalente al UNO POR CIENTO (1%) del monto mensual que correspondería al servicio de soporte hasta un máximo de DIEZ POR CIENTO (10%) por incidente, siendo acumulativos los importes que se hayan imputado debido al atraso en la reparación de otros incidentes del mismo mes.

E. ESPECIFICACIONES TÉCNICAS

"RENOVACIÓN INTEGRAL DE LA INFRAESTRUCTURA DE FIRMA DIGITAL DE LA AUTORIDAD CERTIFICANTE OFICINA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN"

I. INTRODUCCIÓN

El presente documento detalla la solución integral solicitada por el contratante para actualizar la infraestructura de hardware y software de base, infraestructura de redes y firewalls de la Autoridad Certificante de Firma Digital de la ONTI, incluyendo modificaciones y actualizaciones dentro del código de la aplicación existente**.**

II. OBJETO DE LA CONTRATACIÓN

Modernizar integralmente la infraestructura tecnológica de la Autoridad Certificante ONTI, comprendiendo el reemplazo de equipamiento, soluciones de soporte de servidores y de aplicaciones automatizadas y preventivas, y herramientas de software actualizadas e integradas para supervisar el entorno**.**

III. DETALLE DE BIENES Y SERVICIOS

La empresa proveerá una única solución para actualizar tecnologías de virtualización, desarrollo y actualización de software, adquisición de equipamiento, soporte, migración, mejora funcional, transferencia tecnológica y rediseño de arquitectura, que provea una solución activa en producción y contingencia en lo referente a la disponibilidad de la información y la seguridad que aporta.

El sistema informático y el equipamiento actualmente en operación permiten realizar todos los procesos de solicitud, aprobación, emisión y revocación de certificados digitales de acuerdo a los lineamientos de la normativa de Firma Digital Argentina. El desarrollo informático comprende métodos y funcionalidades de criptografía, que permiten la generación de claves en cualquier dispositivo criptográfico. La aplicación se encuentra desarrollada en ".net" con una base de datos "SQL Server".

Los sitios de producción y de contingencia estarán configurados en un esquema denominado ACTIVO-ACTIVO, implementado en dos data centers. Es decir que el sitio de contingencia tendrá una réplica exacta y actualizada en vivo de las operaciones realizadas en el sitio de producción. El sitio de contingencia estará en estado activo (además del sitio de producción), y ambos estarán protegidos mediante un esquema de alta disponibilidad para estar protegido ante la pérdida de algún componente físico de la solución. La solución completa deberá contemplar un escenario de alta disponibilidad, que permita la redundancia de la información y de las tecnologías. La plataforma estará

separada en zonas conectadas desde el punto de vista de la seguridad mediante firewalls de hardware. El proveedor será el responsable de la ejecución de todas las acciones técnicas para la gestión unificada de la solución.

Por otra parte, la experiencia de la adquisición de servidores y switches a diferentes fabricantes en 2010 y 2015 generó inconvenientes de mantenimiento por la diversificación de la interlocución con los fabricantes. Por lo tanto, ambos tipos de equipamientos ofertados deberán ser de la misma marca.

El detalle de los bienes y servicios a adquirir es el siguiente**:**

1.1 Equipamiento

Los equipos serán provistos junto a sus garantías y soportes oficiales de los fabricantes, de acuerdo al siguiente detalle:

1.1.1 Equipamiento de redes

Se adquirirán 4 (cuatro) switches de red, cuyas características técnicas se adjuntan como **Anexo A**

1.1.2. Servidores
Se adquirirán 10 (diez) Servidores de Red Genéricos para Servidores, cuyas especificaciones técnicas se adjuntan como **Anexo B.**

1.1.3 Equipos de seguridad perimetral
Se proveerán 8 equipos de Fire Wall, de acuerdo a las especificaciones técnicas del **Anexo C.**

2. Actualización funcional de la Plataforma para nuevas prestaciones

El objetivo de este servicio es desarrollar un nuevo sistema de emisión y administración del ciclo de vida de los certificados digitales emitidos por la AC ONTI, que requiere la modificación del código de desarrollo de la solución original. Ese sistema contendrá las siguientes nuevas funciones, cuyas especificaciones técnicas se adjuntan como anexos:

generación de certificados para aplicaciones **(Anexo D) ;**

generación de certificados para sitios seguros **(Anexo E); e**

integración con datos biométricos del RENAPER para personas humanas, a fin de permitir la aprobación y renovación remota de certificados digitales con datos biométricos **(Anexo F).**

3. Migración de la Plataforma actualizada a la nueva infraestructura.

Esta actividad crítica consiste en la puesta en operación del equipamiento y la migración de aplicaciones y bases de datos desde la plataforma anterior. Una vez instalado el equipamiento, se migrarán las bases de datos de la aplicación actual a la última versión de

motor de bases de datos y, finalmente, se apuntará la aplicación a estas bases actualizadas para que la nueva Plataforma quede en operación. Luego de la migración de la infraestructura, las condiciones importantes relacionadas con la criticidad del servicio deberán mantenerse o mejorarse.

Esta actividad se realizará de acuerdo al siguiente detalle:

i) Infraestructura de hardware de red:

- Implementación de Dispositivos de Networking;
- Instalación de Switches y Firewalls; Actualización de niveles de Firmware y software de equipamiento de red, generación de política y procedimiento;
- Implementación de controles adicionales sobre protocolo STP (Spanning tree protocol);
- Diseñar e implementar el ruteo entre Sites mediante cambios en las VPN para transportar segmentos de red y no comunicaciones host-to-host;
- Implementación de etherchannels o ports LACP en modo activo-activo para todos los servidores;
- Implementación de port security y control de acceso a las bocas de red; diseño e implementación de Policies de filtrado de los equipos Firewalls Fortigate;
- Implementación de protocolos de gestión encriptados como SSH (actualmente se utiliza telnet); Implementación de hardening adicional de seguridad en equipamiento de red;
- Diseño e implementación de accesos VPN y sus usuarios. Generación de política y procedimiento;
- Scan de seguridad perimetral y generación de informes;
- Mejoras sobre los mecanismos de logging y reportes de los equipos Firewalls Fortigate;
- Implementación de software y procesos de monitoreo, alerting y capacity planning**.**

ii) infraestructura de hardware de servidores:

- Desembalaje, revisión y rackeo del equipo en Rack de 19” existente;
- Conexión física del equipo;
- Inicialización del sistema de almacenamiento provisto;
- Actualización de Firmware (en caso de requerir);
- Alta de equipo en el Soporte oficial;
- Instalación y activación de Licencias (si fuesen adquiridas junto al equipo);
- Pruebas Funcionales.

iii) Infraestructura de hardware de seguridad perimetral:

- Elementos y sistemas electrónicos y mecánicos para la protección de perímetros físicos;
- Detección de tentativas de intrusión
- Detección de malware
- Filtrado de contenido malicioso.

iv) Infraestructura de software Microsoft:

Infraestructura de base: Instalación de Windows Server en Servidores Físicos; Alta del servicio Hyper-V en todos los servidores físicos; Configuración de Hyper-V para soporte de alta disponibilidad; Creación de todas las máquinas virtuales**.**

Arquitectura de dominio: Instalación de Arquitectura de Dominio; Alta de Active Directory Domain Services; Alta de DNS; Alta de DHCP; Diseño y creación de GPO**.**

Infraestructura System Center Configuration Manager: Instalación del Servidor de DB; Instalación del Servidor de Sitio; Instalación de Roles de Distribución de SO; Instalación de Roles de Distribución de Actualizaciones; Creación y prueba de Imagen de Sistemas Operativos; Configuración del esquema de distribución de SO mediante PXE.

Instalación de Sistemas Operativos de Equipos Virtuales mediante SCCM.

Actualización de toda la Infraestructura Windows.

Instalación de pre-requisitos Active Directory: Roles de AD; Infraestructura PKI.

Instalación de Motores de Base de Datos SQL.

Instalación de pre-requistos para servicios de la PLATAFORMA por Servidor.

v) Infraestructura de Backup Veeam: Instalación de Herramienta Veeam Backup; Diseño y Configuración de Metodologías de replicación y Políticas de Retención; Diseño y Configuración de Seteos avanzados (Mantenimiento, Configuraciones de Storage, Notificaciones y Configuraciones de Hyper-V); Creación de Jobs de Backup (Configuración de Jobs de Backup de Dispositivos de Hardware de Red; Configuración de Jobs de Backup de Bases de Datos; Configuración de Jobs de Backup de Configuraciones de Aplicaciones; y Creación de Jobs de Backup de Máquinas Virtuales Críticas).

vi) Infraestructura de Monitoreo: Instalación de pre-requisitos para la herramienta Whatsup Gold; Instalación de la herramienta Whatsup Gold; Configuración de monitoreo (Descubrir dispositivos en la red, Promover dispositivos descubiertos a "Managed Devices", Crear y configurar Monitores), Crear reportes, informes detallados y resúmenes de estadísticas y estados de los dispositivos); Crear Roles de usuario, Políticas y Cadenas de notificación; Automatizar acciones correctivas para manejar alertas y eventos de redes, dispositivos y aplicaciones**.**

vii) Funcionalidades adicionales de monitoreo de la infraestructura de la Plataforma completa (hardware de red, de seguridad perimetral, de servidores, de funcionamiento y estado de salud de sistemas Operativos, funcionamiento y estado de salud de componentes como Active Directory, SQL Server y Hyper-V);

viii) Funcionalidades adicionales de backup de la infraestructura de la Plataforma, incluyendo configuración de los dispositivos de red y seguridad perimetral, bases de datos y configuraciones de la Aplicación de Firma Digital;

ix) dada la posibilidad que otorga el organismo de contar con alojamiento en dos salas cofre diferentes, se duplicarán las infraestructuras para cumplir con la premisa de "Disaster Recovery" ante catástrofe, y permitir así el servicio de continuidad de negocio, duplicando

roles de la Plataforma para que mantenga un alto SLA. Esto implica clusters de Windows Server utilizando Hyper-V, roles duplicados de Active Directory y de la Aplicación de Firma Digital.

4. Capacitación

La actualización del equipamiento y el software de la Plataforma, las nuevas funcionalidades de la aplicación de Firma Digital y las nuevas herramientas de monitoreo y backup, requerirán la capacitación y transferencia tecnológica para aproximadamente diez técnicos y técnicas de nivel intermedio / avanzado de la Oficina Nacional de Tecnologías de Información, y de la Subsecretaría de Innovación Administrativa. Debido a la especificidad de la solución integral que quedará en operación, la empresa deberá brindar al menos cuatro cursos de entrenamiento diseñados específicamente para que los destinatarios puedan realizar todas las tareas requeridas para la administración de la Plataforma. Asimismo, durante todo el proceso de instalación y puesta en operación de la solución, la empresa deberá prestar el asesoramiento técnico que considere oportuno para el mejor aprendizaje del funcionamiento de la nueva Plataforma por parte del personal. Si bien la definición final de los contenidos de los cursos deberá ser previamente acordado con el contratante, se estima que estos deberán contemplar al menos **cuatro sesiones de aproximadamente 6 horas cada uno**, según el siguiente detalle:

i) Administración de Infraestructura de Redes: diseño de la infraestructura implementada, mantenimiento que se brindará sobre los equipos, alertas e incidentes en la herramienta de monitoreo, alertas de seguridad de Firewalls, configuraciones sobre los equipos.

ii) Administración de Infraestructura de Servidores: diseño de la infraestructura implementada; mantenimiento que se brindará sobre los equipos, alertas e incidentes de Hardware de los servidores, configuraciones o actualizaciones sobre los equipos.

iii) Administración de Infraestructura Microsoft: diseño de la infraestructura implementada, diseño de actualización periódica de parches, metodología automática de despliegue de parches y actualizaciones, funcionamiento y seguimiento de alertas, alerta e incidentes en la Plataforma, metodología de Backup, monitoreo (seguimiento de alertas y monitores, configuración de umbrales y escalamiento ante incidentes), Backup (seguimiento de realización de backups, adhesión y quite de servicios en backup, alertas e incidente de backup), configuraciones y actualizaciones sobre la infraestructura.

iv) Administración de la Aplicación de Firma Digital: diseño de la infraestructura implementada, diferencias entre versión anterior y la nueva, nuevas funcionalidades, administración básica de la aplicación, incidentes).

5. Soporte integral

El objetivo de estas tareas es prestar apoyo especializado frente a cualquier contingencia que se pueda presentar en cualquier componente de la Plataforma dentro del contexto de servicio, incluyendo todo el equipamiento de hardware, redes, sistema operativo, software y nuevas funcionalidades. El servicio de soporte tendrá una **duración de 12 meses** corridos

desde la puesta en operación del nuevo equipamiento.

Alcance:

Soporte Reactivo de la Plataforma (análisis, seguimiento y coordinación de todas las actividades relacionadas con la gestión de un incidente o problema, hasta que se dé solución al mismo). Los incidentes de soporte se gestionarán por Portal Web, correo electrónico o por teléfono. Una vez generado el incidente de soporte por cualquiera de los medios disponibles, será asignado de manera automática un número ID de caso, con el cual se podrá realizar el seguimiento respectivo a través del Portal Web. En caso de ser requerido se podrá modificar el nivel de severidad y el nivel de escalamiento que corresponda, mientras que la empresa deberá determinar la cantidad y perfil de recursos a asignar para la resolución de cada incidente. Cabe aclarar que, dado que el proveedor deberá adquirir el equipamiento, deberá incluirse en el servicio de soporte un esquema de escalamiento con los distintos fabricantes (tanto de Software como de Hardware), y presentar los esquemas de garantías de hardware adquirido, incluyendo el soporte del fabricante on site por tres años (fallas de servidor, rotura de discos, fuentes de servidor, etc.), y la actualización de garantía básica por instalación in situ de todas las piezas de repuesto. En todos los casos en que se reemplacen discos por fallas, el contratante retendrá los defectuosos**.**

Soporte Evolutivo: tareas de tecnología preventiva, capacitaciones, transferencia de conocimiento, asesoramiento sobre temas puntuales y evaluación de alternativas sobre nuevas aplicaciones. Todas estas tareas excluyen la implementación que requiera el desarrollo del diseño de una solución específica, y la implementación de ningún tipo de tecnología que requiera un diseño específico para una solución particular**.**

Disponibilidad:

Los incidentes de soporte se realizarán vía web, correo electrónico y telefónico, con seguimiento web de la respuesta. Será responsabilidad del proveedor determinar la cantidad y perfil de recursos a asignar para la resolución de dicho incidente. El proveedor deberá disponer de un correo electrónico y un número telefónico destinado al reporte de incidentes, con **disponibilidad 24 x 7.**

Tiempo de Respuesta: tiempo transcurrido entre la comunicación al proveedor de la existencia del mal funcionamiento del/los componente/s (llamada de servicio) hasta que el mismo toma contacto a los efectos de iniciar el tratamiento del incidente.

Tiempo de Reparación: tiempo transcurrido entre la toma de contacto entre el cliente y el proveedor ante una incidencia hasta la corrección de la misma y puesta en funcionamiento a satisfacción del cliente**.**

Reparación: se entiende que el componente reparado funcione u opere en las mismas condiciones previas al incidente**.**

Para el cumplimiento de lo estipulado, se entenderá como **incidente**: a cualquier desperfecto, funcionamiento anormal, o fuera de servicio parcial o total; a cualquier tipo y clase de evento que no permita que se pueda cumplir con el desempeño deseado según las especificaciones técnicas y/o funcionales realizadas**.**

A su vez, estos se dividen según su criticidad:

Criticidad Alta: esta condición de servicio es válida cuando todos los usuarios son afectados o, dada la caída de un sistema crítico para el negocio, el impacto organizacional es alto.

Criticidad Media: condición válida cuando existe una degradación significativa en el rendimiento del servicio productivo.

Criticidad Baja: válida para casos en que no se presentan usuarios afectados, y se asocia a un requerimiento de cambios de configuración con el fin de aumentar la performance o para seguir una normativa establecida**.**

Los niveles de servicio se definen por los tiempos de respuesta máximos acordados de acuerdo a la criticidad de los incidentes que pudieran surgir**:**

Criticidad Alta: Tiempo máximo de respuesta: UNA (1) hora, con disponibilidad de lunes a domingo (7 x 24). Tiempo de resolución máximo: SEIS (6) horas corridas**;**

Criticidad Media: Tiempo máximo de respuesta: SEIS (6) horas, con disponibilidad 5 x 9 en el horario comprendido entre las 9:00 y las 18:00. Tiempo de resolución máximo: CUARENTA Y OCHO (48) horas corridas**;**

Criticidad Baja: Tiempo máximo de respuesta a programar con el contratante, con disponibilidad 5 x 9 en el horario comprendido entre las 9:00 y las 18:00. Tiempo de resolución máximo: SIETE (7) días corridos**.**

<u>Continuidad de la plataforma</u>:
El proveedor deberá proveer los manuales y procedimientos necesarios para que el área requirente pueda poner en funcionamiento el servicio y resolver los posibles errores comunes. Todos los incidentes indicados por el área requirente y resueltos por el proveedor, deben ser documentados, de manera de permitir a futuro al área requirente la resolución del incidente en caso de que vuelva a surgir. El proveedor se compromete a realizar los mejores esfuerzos técnicos y profesionales que tiene a su disposición, a fin de asegurar la transferencia de conocimiento al área requirente para operar la infraestructura, de manera que una vez que finalice el soporte técnico, el área requirente pueda mantener el nivel de servicio en los valores requeridos.

.

ANEXO A

SWITCHES DE RED

1. Se proveerán 4 (cuatro) equipos con 36 meses de garantía y soporte del fabricante.

2. El equipo debe soportar Fuentes de poder redundante y hot-swap.

3. Los switches a proveer deben estar basados en una conexión de al menos 10Gb entre los switches y los servidores.

4. Debe permitir Virtual Link Aggregation con puertos de 40 Gb y usar para la redundancia al menos dos en forma activo/activo.

5. Los switches deben contar con fuentes redundantes y ventiladores hotswap

6. Los switches deben tener al menos la siguiente distribución de puertos: 48 Puertos de al menos 10Gb. Debe permitir el acceso a la interfaz física mediante transceptores enchufables del tipo SFP o SFP+ o similar.

7. Deberán contar con una velocidad de conmutación inicial sin bloqueos, no inferior a la sumatoria del ancho de banda de todos los puertos solicitados en la configuración inicial, considerando que los mismos operan en modo full-duplex. Deberán contar con soporte de Jumbo Frames de al menos 9000 bytes de longitud.

8. Los switches deben contar con un sistema operativo basado en solución de Cloud que soporte almenos los siguientes puntos: 802.1AB, 802.1D, 802.1s, 802.1w, 802.1Q, 802.3ad, virtual LAG (vLAG), 802.1Qbb PFC, CEE, 802.1Qaz ETS, Telnet interface for CLI, Secure FTP (sFTP), Network Time Protocol (NTP) for switch clock synchronization, IPv4/IPv6 management, IPv4/IPv6 routing, DHCP Relay, IPv4/IPv6 virtual router redundancy protocol (VRRP), Border Gateway Protocol (BGP) Automation: Zero Touch Provisioning, Python APIs, REST APIs ONIE-enabled, Port mirroring for analyzing network traffic passing through switch, Service Location Protocol (SLP) Secure Shell (SSH), User Access Control, VLAN-based, MAC-based, and IP-based access control lists (ACLs), Egress ACLs, TACACS+, RADIUS.
9. Se prefiere que los switches de la solución sean del mismo fabricante de los nodos/servidores ofertados con el fin de que el soporte sea sobre toda la solución

.

ANEXO B
SERVIDORES DE RED

- ✓ Se proveerán 10 (diez) equipos con 36 meses de garantía y soporte del fabricante.
- ✓ Deberá ser totalmente compatible con Arquitectura X86.
- ✓ Deberá poseer setup residente en ROM, CD-ROM o DVD-ROM con password de ingreso y encendido.
- ✓ Deberá poseer control de booteo residente en ROM, con posibilidad de booteo desde CD-ROM y/o DVD-ROM.
- ✓ Deberá poseer reloj en tiempo real con batería y alarma audible.
- ✓ Deberán indicarse otros controles adicionales que posea.

UNIDAD CENTRAL DE PROCESO

- ✓ El procesador debe poseer 16 cores a 2.3GHz como mínimo, cache de 22MB como mínimo y debe ser de última generación con fecha de lanzamiento al mercado no anterior a 2019.
- ✓ Cantidad de sockets a proveer (cada socket soportará la instalación de 1 CPU del tipo seleccionado): al menos 2 (dos)
- ✓ Cantidad de CPU a proveer instaladas (para el tipo seleccionado): al menos 2 (dos)

MEMORIA RAM A PROVEER Y SU ESCALABILIDAD

- ✓ Tipo de memoria: DDR4 con corrección de errores (ECC).
- ✓ Capacidad:

Capacidad inicial	*Máxima instalable (valor mínimo)*
128 GB	512 Gb

PUERTOS INCORPORADOS

- ✓ Se deberán proveer los siguientes puertos:
  - 1 (uno) Port para mouse tipo USB
  - 1 (uno) Port para teclado tipo USB
  - 1 (uno) Port para monitor
  - Al menos 1 (uno) Puertos USB (Universal Serial Bus) versión 2.0
  - Al menos 3 (tres) Puertos USB (Universal Serial Bus) versión 3.0
  - Al menos 1 (uno) Puertos D-Sub 15

NETWORKING Y COMUNICACIONES

- ✓ En la tabla de abajo se indican las interfaces de red que se deberán proveer:

TIPO DE INTERFAZ	CANTIDAD DE PUERTOS (MÍNIMO)
❑ Puerto 1 Gigabit Ethernet en cobre (RJ45) para administración remota	1 (uno)
❑ Puerto 10 Gigabit Ethernet SFP+ (debe incluir transceiver SR)	2 (dos)

BUS DE E/S Y EXPANSIÓN

- ✓ Bus de E/S: Deberá soportar mínimamente los estándares PCIe 3.0
- ✓ Expansión: Luego de instaladas todas las placas PCI necesarias para cubrir las características del equipo solicitado, deberán quedar: 2 slot PCIe 3.0 libres para futuras ampliaciones.

ADAPTADOR DE VIDEO

- ✓ VGA o superior con 8MB de memoria mínimo para soporte de las interfaces gráficas de los sistemas operativos existentes en el mercado.

ACCESORIOS

- ✓ Debe ser Rackeable, incluyendo todos los accesorios, tornillos y elementos necesarios para ser alojado en un rack de 19" estándar.
- ✓ No debe ocupar más de 1 (una) unidad de Rack.

ALMACENAMIENTO MASIVO INTERNO:

- ✓ **Característica de la CONTROLADORA DE DISCOS DUROS:**
  - Tipo:
    SAS y SATA: El conjunto formado por la controladora de disco y la/s unidad/es de disco/s, deberán transferir hacia el canal SAS/SATA a una tasa sincrónica no inferior a 6.0 Gbps.
    HOT-SWAP: La controladora de discos duros, así como los discos usados en la implementación del sistema de almacenamiento masivo deberán soportar capacidad Hot-Swap de los discos.
  - Configuraciones RAID soportadas: RAID 0, 1, 10, 5, 50, 6 y 60 por hardware en todos los canales.
  - Cache: 2 GB de memoria cache no volátil como mínimo.

- ✓ **DISCOS DUROS que componen el almacenamiento interno:**
  - 2 (dos) discos con una capacidad de al menos 240 GB SSD HotSwap SATA 6 Gb/s
  - 3 (tres) discos con una capacidad de al menos 2.4 TB 10.000 rpm HotSwap SAS 12 Gb/s
  - Debe tener capacidad para soportar al menos 8 discos sin realizar modificaciones en el equipo.

- ✓ **Configuración del almacenamiento interno:**
  - Configuración RAID a proveer en el conjunto de discos:

    RAID 1 (Mirroring) para los discos SATA SSD para el SO

    RAID 5 (Data Stripping with parity) para los discos SAS de datos.

FUENTE DE ALIMENTACIÓN

- ✓ Deberá poder conectarse directamente a la red de suministro de energía eléctrica de 220 V, además de tener conexión a tierra.
- ✓ De al menos 1100 watts c/u
- ✓ Con tecnología Hot-swap.
- ✓ La fuente de alimentación debe ser redundante del tipo N+1.

SISTEMA OPERATIVO

- ✓ No se provee pero debe ser compatible con: Microsoft, SUSE, Red Hat y VMware vSphere.

ALMACENAMIENTO EXTRAIBLE

- ✓ Medios ópticos:

  Se deben proveer 2 (dos) Lectograbadora de DVD-R/RW USB externas en total (una para cada sitio)

ANEXO C

EQUIPAMIENTO DE ADMINISTRACIÓN UNIFICADA DE AMENAZAS

Se proveerán 8 (ocho) equipos con 36 meses de garantía y soporte del fabricante.

El Sistema de seguridad informática perimetral será del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), donde se deberán ofrecer ya incluidas y listas para ser utilizadas, las funcionalidades que se detallan a continuación.

- El dispositivo debe ser un equipo de propósito específico, basado en tecnología ASIC. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers) sobre los cuales pueda instalarse y/o ejecutar un sistema operativo regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
- Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).
- Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).
- El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
- El sistema operativo debe incluir un servidor de DNS que permita resolver consultas locales.
- El equipo debe soportar el uso del protocolo ICAP con el fin de poder delegar tareas a equipos terceros con el fin de liberar procesamiento del mismo.
- Las reglas de firewall deben analizar las conexiones que atraviesen el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- El firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo, y en base a fechas (incluyendo día, mes y año)
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.

- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario)
- Deberá tener la capacidad de balancear carga entre servidores, mediante traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas. Deberá soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID. Deben soportarse mecanismos para detectar la disponibilidad de los servidores.
- Deberá permitir la creación de políticas de tipo Firewall con capacidad de seleccionar campos como dirección, identificador de usuarios o identificador de dispositivos para el caso de dispositivos móviles como smartphones y tabletas.
- Deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN
- Capacidad de hacer captura de paquetes por política de seguridad implementada y exportar en formato PCAP.
- Deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada
- Será capaz de integrar servicios dentro de categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente
- El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas
- Será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si se cuenta con estos procesadores
- Podrá crear e implementar políticas de tipo Multicast y determinar el sentido de la política, así como también la habilitación del NAT dentro de cada interface del dispositivo
- Será capaz de crear e integrar políticas contra ataques DoS, aplicables por interfaces.
- Deberá generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS
- Permitirá configurar el mapeo de protocolos a puertos de manera global o especifica
- Configurará el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
- Integrará la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados
- El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico
- Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis
- La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH

CONECTIVIDAD Y SISTEMA DE RUTEO

- Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.
- Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.

- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- Soporte a políticas de ruteo (policy routing).
- El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir qué tráfico sale por un enlace y qué tráfico sale por otro enlace
- Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS
- Soporte a ruteo dinámico RIPng, OSPFv3
- La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.
- Soporte de ECMP (Equal Cost Multi-Path) con peso, el tráfico será distribuido entre múltiples rutas pero en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento, el tráfico será enviado de acuerdo a la definición de una ruta hasta que se alcance un umbral de tráfico. En este punto se comenzará a utilizar en paralelo una ruta alternativa.
- Soporte a ruteo de multicast
- Permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
- Podrá habilitar políticas de ruteo en IPv6
- Deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6
- Deberá soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario, con IPv6
- La solución será capaz de habilitar funcionalidades de UTM (Antivirus, Filtrado Web, Control de Aplicaciones, IPS,Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas con direccionamiento IPv6
- El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6
- El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explicito
- Deberá ser capaz de integrar políticas con proxy explícito en IPv6
- La solución podrá restringir direcciones IPv6 en modo proxy explicito
- Deberá hacer NAT de la red en IPv6
- La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT
- Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo
- Deberá ser capaz de habilitar políticas de seguridad con funcionalidades IPS, Filtrado Web, Control de Aplicaciones, Antivirus y DLP, para la inspección de tráfico en IPv6 basado en flujos
- La solución contara con una base de administración de información interna generada por sesiones sobre IPv6
- Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6
- El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6
- Tendrá la funcionalidad de habilitar DHCP en IPv6 por interface
- Contará con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad
- El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrara el archivo de configuración

- El dispositivo podrá hacer la función como servidor DHCP IPv6
- La solución será capaz de configurar la autenticación por usuario por interface en IPv6

VPN IPSec/L2TP/PPTP

- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)
- Soporte para IKEv2 y IKE Configuration Method
- Debe soportar la configuración de túneles PPTP
- Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.
- Soportará longitudes de llave para AES de 128, 192 y 256 bits
- Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
- Soportará los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's IPSeC site-to-site y VPNs IPSec client-to-site.
- La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN), en ese modo la VPN IPSec deberá poder asignar una dirección IP, asignar rutas para ser encaminadas por esta interface y estar presente como interface fuente o destino en políticas de firewall.
- Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

VPN SSL

- Capacidad de realizar SSL VPNs.
- Soporte a certificados PKI X.509 para construcción de VPNs SSL.
- Soporte de autenticación de dos factores. el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
- Soporte de renovación de contraseñas para LDAP y RADIUS.
- Soporte a asignación de aplicaciones permitidas por grupo de usuarios
- Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.
- Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
- Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)
- La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS
- Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
- Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
- Los portales personalizados deberán soportar al menos la definición de:
  - Widgets a mostrar

- Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC
- Esquema de colores
- Soporte para Escritorio Virtual
- Política de verificación de la estación de trabajo.

- La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, o sea un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.
- Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN SSL debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.

Traffic Shapping / QoS

- Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall
- Asignación de parámetros de traffic shaping diferenciados para el tráfico en distintos sentidos de una misma sesión, para cada dirección IP en forma independiente y los mismos para la regla en general.
- Capacidad de poder definir ancho de banda garantizado y límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo
- Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia

AUTENTICACIÓN Y CERTIFICACIÓN DIGITAL

- Capacidad de integrarse con Servidores de Autenticación RADIUS.
- Capacidad nativa de integrarse con directorios LDAP
- Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios aprovechando las credenciales existentes "Single-Sign-On"
- Autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.
- Posibilidad de definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)
- La solución soportará políticas basadas en identidad, pudiendo definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
- Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
- Política mínima de contraseñas para administradores locales:
  - Longitud mínima permitida
  - Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
  - Expiración de contraseña.
- Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

ANTIVIRUS

- Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
- El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.
- Antivirus en tiempo real, integrado a la plataforma de seguridad. Sin necesidad de instalar un servidor externo, licenciamiento de un producto o software adicional para realizar la categorización del contenido.
- El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.
- La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo, y que permita la aplicación de esta protección por política de control de acceso.
- El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
- El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos.
- El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP
- El Antivirus integrado tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.
- El Antivirus deberá incluír capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
- El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.
- El antivirus deberá ser capaz de filtrar archivos por extensión
- El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo
- Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (recibir las actualizaciones de los centros de actualización sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)

ANTISPAM

- La capacidad antispam incluída deberá detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
- La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear), las cuales podrán ser por dirección IP o por dirección de correo electrónico.

- La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM
- Para SMTP, los mensajes SPAM podrán ser etiquetados o rechazados (descartados). Al etiquetarse, debe poder hacerse en motivo (subject) del mensaje o en un encabezado MIME en el mensaje.

FILTRAJE DE URLS (URL FILTERING)

- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs se debe poder implementar por Categorías y por sitios web.
- Debe poder categorizar contenido Web requerido mediante IPv6.
- Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.
- Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida
- La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión (modo proxy) como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación (modo flujo).
- Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, por denegación) deberán ser personalizables. Estos mensajes de reemplazo deberán poder aplicarse para conexiones http y https, tanto en modo proxy como en modo flujo.
- Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido.
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- La solución de Filtrado de Contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Google, Yahoo! y Bing.
- Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
- Será posible exceptuar la inspección de HTTPS por categoría.
- Debe contar con la capacidad de implementar el filtro de Educacion de Youtube por Perfil de Filtro de Contenido para trafico HTTP, garantizando de manera centralizada, que todas las sesiones aceptadas por una política de seguridad con este perfil, van a poder acceder solamente a contenido de tipo Educativo en Youtbube.
- El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección:
- 1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir.
- 2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.

- 3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado.
- Se debe incluir la funcionalidad de reputación basada en filtrado de URLs. Al acceder a páginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigna un puntaje a cada usuario o IP. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con el fin de detectar zombies dentro de la red.
- Capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.
- Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)
- En dicho sistema cada organismo obtiene un ID de Youtube para habilitar el contenido educativo del mismo. Se deberá insertar dicho codigo en la configuración de filtrado de URLs del equipo para poder habilitar unicamente el contenido educativo de Youtube.

PROTECCIÓN CONTRA INTRUSOS (IPS)

- El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror.
- Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.
- Capacidad de detección de más de 4000 ataques.
- Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (recibir las actualizaciones de los centros de actualización sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)
- El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos.
- La interfaz de administración del detector y preventor de intrusos deberá estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
- El detector y preventor de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).
- Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
- Actualización automática de firmas para el detector de intrusos
- El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.

- Métodos de notificación:
  - Alarmas mostradas en la consola de administración del appliance.

- Alertas vía correo electrónico.
- Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
- La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico o de forma "indefinida", hasta que un administrador tome una acción al respecto.
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.

- Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir:
  - Protección contra botnets: Se deben bloquear intentos de conexión a servidores de Botnets, para ello se debe contar con una lista de los servidores de Botnet más utilizado. Dicha lista debe actualizarse de forma periodica por el fabricante.

  - Sandboxing: La funcionalidad de Sandbox hace que el archivo sea ejecutado en un ambiente seguro para analizar su comportamiento y, a base del mismo, tomar una acción sobre el mismo.

PREVENCIÓN DE FUGA DE INFORMACIÓN (DLP)

- La solución debe ofrecer la posibilidad de definir reglas que permitan analizar los distintos archivos que circulan a través de la red en búsqueda de información confidencial.
- Debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.
- Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.
- Ante detección de posible fuga de información deben poder aplicarse las siguientes acciones: Bloquear el tráfico del usuario, Bloquear el tráfico de la dirección IP de origen, registrar el evento,
- En caso del bloqueo de usuarios, debe permitir definir por cuánto tiempo se hará el bloqueo o en su defecto bloquear por tiempo indefinido hasta que el administrador tome una acción.
- La solución debe soportar la capacidad de guardar una copia del archivo identificado como posible fuga de información. Esta copia podría ser archivada localmente o en otro dispositivo.
- La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.
- Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes:
  - Filtrado por tipo de archivo
  - Filtrado por nombre de archivo
  - Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.

- Fingerprinting: Se tomará muestra del archivo que se considere confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.
- Watermarking: Se insertará un "sello de agua" dentro del archivo considerado como confidencial. De acuerdo a esto se analizarán los archivos en busca de este sello de agua, este se detectará incluso si el archivo sufrió cambios.

CONTROL DE APLICACIONES

- Debe identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
- La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.
- El listado de aplicaciones debe actualizarse periódicamente.
- Para aplicaciones identificadas deben definirse opciones: permitir, bloquear, registrar en log.
- Para aplicaciones no identificadas deben definirse opciones: permitir, bloquear, registrar en log.
- Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
- Preferentemente deben soportar mayor granularidad en las acciones.

INSPECCIÓN DE CONTENIDO SSL

- La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
- La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
- La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
- Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
- El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS

FILTRADO DE TRÁFICO VOIP, PEER-TO-PEER Y MENSAJERÍA INSTANTÁNEA

- Soporte a aplicaciones multimedia tales, como mínimo: SCCP(Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).
- El dispositivo tendrá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer.

- Para programas de compartir archivos (peer-to-peer) limitará el ancho de banda utilizado por ellos, de manera individual.
- La solución debe contar con un ALG (Application Layer Gateway) de SIP
- Debe poder hacer inspección de encabezados de SIP
- Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP.
- La solución debe soportar SIP HNT (Hosted NAT Transversal).
- La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes
- Deberá ser capaz de hacer inspección de tráfico SSH en modo proxy explicito
- La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo
- El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS

OPTIMIZACIÓN WAN Y WEB CACHING

- Deberá permitir la creación de perfiles para la aplicación de Optimización WAN e indicar bajo que protocolos se ejecutara
- Deberá ser capaz de activar en modo transparente dentro de los perfiles de Optimización WAN y seleccionar un determinado grupo de usuarios para autenticación de acceso
- El dispositivo deberá soportar la desfragmentación dinámica de paquetes para detectar fragmentos persistentes de distintos archivos o datos adjuntos dentro del trafico bajo protocolos desconocidos
- La solución debe ser capaz de generar y aplicar perfiles de Optimización WAN para los usuarios
- El dispositivo de seguridad podrá integrar contenido de inspección dentro de sus políticas de seguridad con Optimización WAN
- La solución integrara dentro de cada interface capacidad de hacer túneles de Optimización WAN
- Deberá ser capaz de configurar Optimización WAN en modo Activo/Pasivo
- Solución capaz de aplicar web cache a tráfico HTTP y HTTPS dentro de las políticas de seguridad incluyendo también Optimización WAN y web proxy cache
- Dispositivo capaz de habilitar el almacenamiento en caché web tanto en el lado del cliente y del lado de la solución
- La solución podrá recibir el tráfico HTTPS en nombre del cliente, abrirá y extraerá el contenido del tráfico cifrado para inspeccionar y almacenar en cache para el envío al usuario final
- El dispositivo tendrá la opción de integrar un certificado SSL determinado para la recifrado de tráfico
- La solución capaz de configurar el cache de trafico HTTP y HTTPS bajo distintos puertos a los predeterminados (80 y 443)
- La solución debe ser capaz de habilitar opciones para depurar la funcionalidad de Web Cache a determinadas URL

ALTA DISPONIBILIDAD

- El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6
- Alta Disponibilidad en modo Activo-Pasivo y Activo-Activo
- Posibilidad de definir al menos dos interfaces para sincronía
- El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red
- Será posible definir interfaces de gestión independientes para cada miembro en un clúster.

CARACTERÍSTICAS DE ADMINISTRACIÓN

- Interfase gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad, parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS)
- La interfase gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.
- Interfase basada en línea de comando (CLI) para administración de la solución.
- Puerto serial dedicado para administración, etiquetado e identificado para tal efecto.
- Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)
- El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.
- Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.
- El equipo ofrecerá la flexibilidad para que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.
- El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y logs) desde cualquier equipo conectado a la red que tenga un web browser instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2 y 3
- Soporte de al menos 3 servidores syslog remotos para poder enviar logs
- Posible almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.
- Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
- Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP ante un evento relevante para la correcta operación de la red.
- Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
- Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.

- Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho y ayudantes de configuración (setup wizard).
- Contar con la posibilidad de agregar una barra superior (Top Bar) cuando los usuarios estén navegando con información como el ID de usuario, cuota de navegación utilizada, y aplicaciones que vayan en contra de las políticas de la empresa.
- Herramientas gráficas para visualizar las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos: Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

VIRTUALIZACIÓN

- Deberá poder virtualizar servicios de seguridad mediante "Virtual Systems, Firewalls o Domains"
- La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus
- Debe incluir la licencia para al menos 8 (ocho) instancias virtuales redundantes dentro del equipo.
- Cada instancia virtual debe poder tener un administrador independiente
- La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
- Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red
- Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual
- Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
- Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.
- Definición de comunicación entre los sistemas virtuales internamente sin que el tráfico salga del equipo por medio de conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.

LICENCIAMIENTO Y ACTUALIZACIONES DE PLATAFORMA

- La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD
- El dispositivo tendrá la opción de conectarse a los servidores NTP de los Laboratorios de Investigación y Actualización propietarios del mismo fabricante para actualización del horario de sistema local
- Sera capaz de hacer consultas a los servidores DNS de los Laboratorios de Investigación y Actualización del mismo fabricante para resolución y categorización de sitios web dentro de los perfiles para Filtrado Web
- Tendrá la capacidad de hacer consultas a los servidores DNS de los Laboratorios de investigación y Actualización mismos del fabricante sobre reputación de direcciones IP

- El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo.
- La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos 36 meses.

DESEMPEÑO / CONECTIVIDAD

- Los equipos deben por lo menos ofrecer las siguientes características de desempeño y conectividad que surgirán del relevamiento de la visita del oferente a obra.

	Características
Numero de Interfaces Requeridas	16 x GE RJ45 con 16 x GE SFP
Throughput de Firewall	32 Gbps
Throughput de VPN IPSec	20 Gbps
Throughput de Threat Protection	3 Gbps
Throughput de IPS	5 Gbps
Tuneles dedicados	2000
Tuneles SSL	500
Throughput VPN SSL	2.5 Gbps
Sesiones Concurrentes	4.000.000
Nuevas sesiones / segundo	300.000
Politicas del Firewall	10.000
Dimensiones de Rack	1 RU
AC Power	Redundante

- Se deberá incluir un workshop en instalación del Organismo sobre los puntos establecidos de configuración específica, indicando duración del mismo.
- Incluirá servicio de instalación y configuración, así como documentación final.
- El servicio postventa deberá ser en modalidad 7 x 24 telefónico, partes entregadas en domicilio del cliente durante 36 meses y con la mano de obra en sitio incluida para la realización de los cambios necesarios. El tiempo de respuesta deberá ser de 4 hs. luego de registrado el incidente.

ADMINISTRACIÓN CENTRALIZADA

- Sistema de gerenciamiento centralizado que realice aprovisionamiento basado en políticas, configuración de los dispositivos, gerenciamiento de actualizaciones, monitoreo y control de dispositivos de seguridad provistos en este llamado. Por razones de compatibilidad deberá ser de la misma marca de los dispositivos ofertados

FUNCIONALIDADES:

- Centralización de Configuración y monitoreo de todos los dispositivos de seguridad UTM, así como todas sus funciones de protección de red

- Deberá correr sobre entorno virtualizado.
- Se podrán administrar dispositivos “virtuales” que residen en una misma unidad física, como si fuesen un dispositivo completamente independiente dentro de la consola, con su propia configuración y administración.
- Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos.
- Tener un solo repositorio de almacenamiento centralizado y administración de configuraciones, para simplificar las tareas de administración de una gran cantidad de dispositivos de seguridad con protección completa de contenido.
- Las comunicaciones entre la consola de administración y los dispositivos administrados deberán ser cifradas
- La interface de administración deber estar basada en Web Seguro (HTTPS)
- Para un eficiente almacenamiento de las configuraciones, debe incluirse una base de datos relacional integrada compatible con la solución.
- Administración basada en roles para permitir a los administradores delegar los derechos a dispositivos específicos con los privilegios adecuados de lectura/escritura.
- Configuración basada en scripts para flexibilidad y control, automatizando tareas operativas
- Realizar automatización calendarizada de respaldos de configuración y logs.
- Deberá realizar operaciones sobre grupos de dispositivos, y añadir/cambiar/borrar dispositivos a esos grupos.
- Permitir guardado local de actualizaciones de firmas de AV / IPS, filtrado de contenido web y Antispam, con la finalidad de disminuir el tráfico de consultas de actualizaciones a Internet al mínimo y optimizando su uso.
- Soportar conexión a un dispositivo externo de almacenamiento y procesamiento de bitácoras en tiempo real, para solicitar reportes en línea, con una interfaz de administración completamente integrada.
- Crear, exportar y almacenar versiones de configuración de los dispositivos administrados, antes de aplicar cambios a un dispositivo, evitando errores operativos.
- Incluir subsistema monitoreo en tiempo real, para obtener el estado actual de dispositivos administrados, y permitir actuar proactivamente ante un evento de seguridad y operación de los dispositivos de seguridad administrados.
- Administrar el firmware de los dispositivos de seguridad, permitiendo programar y aplicar actualizaciones de sistema operativo de forma desatendida a un equipo o grupo de equipos.
- Permitir configuración en Alta Disponibilidad, de tal forma que en caso de falla pueda existir otro equipo en línea que tome las tareas del equipo dañado con una pérdida mínima en la disponibilidad del servicio.
- Capacidad de creación y aplicación de configuraciones de VPN entre los dispositivos de seguridad administrados.
- Subsistema de monitoreo para los túneles de VPN para unificación desde una sola pantalla el estado de los túneles de VPN.
- Debe de tener la capacidad de aprovisionar y monitorear dispositivos OTP (tokens) en cualquier dispositivo que administre.
- En alta disponibilidad, con dos consolas funcionando en activo/pasivo, los cambios de activo a pasivo deben realizarse sin la necesidad de reiniciar las consolas
- Los administradores deben poder ingresar con su usuario y contraseña a la consola por los protocolos HTTP, HTTPS, SSH y TELNET desde direcciones IPv4 o IPv6

- La consola debe de tener la capacidad de generar reportes basado en los logs enviados por los dispositivos administrados, dichos logs deben poder almacenarse en una base de datos SQL
- Debe poseer esquemas de reportes pre-configurados de todas las funcionabilidades de los dispositivos administrados, pero además realizar reportes 100% personalizados
- La consola debe de tener la posibilidad de recibir o entregar información de los dispositivos administrados, vía APIs para que los mismos puedan ser consultados y/o configurados.
- La administración de las políticas de seguridad de los dispositivos gerenciados debe de tener la facilidad de poder modificarlas con un "drag and drop" en la interface gráfica
- Capacidad de administrar al menos 10 dispositivos iniciales, con crecimiento como mínimo hasta 100 dispositivos sólo con licencias

CONSOLIDACIÓN DE LOGS Y ADMINISTRACIÓN DE REPORTES.

- Sistema de reporte, análisis y almacenamiento de logs, que incluya capacidades de correlación y análisis de vulnerabilidades en la red para dispositivos de Administración Unificada de Amenazas (UTM por sus siglas en inglés) provistos en esta solicitud. Por razones de compatibilidad deberá ser de la misma marca de los dispositivos ofertados.
- La solución propuesta deberá cumplir con las siguientes funcionalidades:
  - Almacenamiento de Logs y Reportes.
  - Sistema operativo propietario
  - Debe implementarse sobre ambientes virtuales, pero en modo appliance
  - Interface de administración gráfica (GUI) vía Web (HTTPS), vía CLI (Línea de comando), vía ssh y consola serial
  - Permitir la definición de dominios administrativos independientes para dividir o segmentar el control de la información recibida y almacenada por dispositivo.
  - Tener la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas
  - Posibilidad de utilizar repositorio de datos externos (bases de datos)
  - Integrar dispositivos para que reporten, y establezcan comunicaciones seguras con dichos dispositivos
  - Asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución
  - Todas las funciones están consolidadas en el dispositivo y/o debe además ofrecer la posibilidad de ser una solución de arquitectura escalable, mediante la asignación de roles específicos o modos de operación a los componentes de la solución (recolector y/o analizador), para optimizar así el manejo y el procesamiento de los logs.

GENERACIÓN DE REPORTES:

- Generar reportes personalizados, el administrador de la solución podrá determinar el contenido de los reportes.

- El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart)
- Generar reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.
- Generar reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.
- Generar reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.
- Incidencia de virus detectados/removidos a nivel red por fuente y/o por destino.
- Reporte de las actividades administrativas realizadas.
- Personalizar los criterios bajo los cuales será obtenido el reporte (origen, destino, servicios, fechas y/o día de la semana).
- Permitir especificar el período específico del reporte, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año).
- Generar reportes mínimamente en formato PDF y TXT, extraíble a Base de Datos seleccionables.
- Generar reportes en idioma español y/o inglés.
- Opcional: Envío del reporte vía correo electrónico.
- Hacer búsquedas por nombre usuario o dirección IP.
- Deberá hacer análisis de vulnerabilidades y generar un reporte, sin tener límite de equipos a analizar.

ALMACENAMIENTO DE CONTENIDO:

- Permite recibir bitácoras de los protocolos http, SMTP para poder almacenar los mensajes que han fluido en la red a través de dichos protocolos, para su posterior visualización
- Los mensajes pueden ser almacenados completamente, o solo un "resumen" de la conexión. El mensaje completo exhibirá el contenido completo, mientras que el resumen solo mostrará fuente y destino de la comunicación, así como su duración.
- Permite hacer búsquedas sobre los mensajes almacenados

ANEXO D

SERVICIO DE GENERACIÓN DE CERTIFICADOS DE APLICACIONES

Certificados de Aplicaciones
Los certificados de firma digital para aplicaciones se emiten para su uso en aplicaciones que realizan firmas digitales automáticamente sin la intervención de un usuario. En general son utilizadas por gestores documentales que firman los documentos recibidos como prueba de su integridad.

Arquitectura
La solución encargada debe estar dividida en distintos Front End, uno por Rol. Cada uno de los front end se deberá construir en .Net Framework, con una arquitectura con separación física de capas mediante servicios WFC. La lógica y validaciones deber encontrarse en un core separado que será el encargado de la persistencia de los datos.

Roles
Se deberá contar con nuevos roles en la aplicación:

- Responsable de certificados de Aplicación
- Gestores de certificados de Aplicación
- Oficiales de Registro de Aplicación

Los pasos para la operación serán los siguientes:

a) PASO 1a: ABM de gestores de aplicación

Condiciones generales:

- El rol que podrá realizar este proceso será el *RESPONSABLE DE CERTIFICADOS DE APLICACIÓN*.

Procedimiento alta:

1. El responsable de certificados de aplicación ingresa al menú de "Administración de gestores de certificados de aplicación".

2. Selecciona la opción para dar de alta un gestor.

3. La aplicación muestra un formulario que le permite ingresar los siguientes datos:

    i. **Persona Autorizante:**
    Aquí se podrá seleccionar una Unidad Operativa (relacionada a la persona autorizante) precargada en el sistema. Si no existe, se deberá poder lanzar

el ABM correspondiente.

- En principio deberá existir:

i. un ABM de Entidades (Organismos padres) con los siguientes datos para cargar: Nombre de organismo, CUIT.

ii. un ABM de **personas autorizantes (unidades operativas)** con los siguientes datos para cargar: Seleccionar organismo padre y nombre de la unidad operativa. También se deberá poder indicar si la designación fue realizada por persona humana o persona Jurídica. De ser el caso de persona humana el sistema permitirá cargar CUIL, Nombre, Apellido y Mail; en el caso que sea persona Jurídica se deberá poder cargar el nombre de la misma, los datos del Nombre, apellido, CUIL y relación vinculante.

- Es importante destacar que si se actualiza el nombre de una unidad operativa se debe indicar quien hizo la designación como se menciona en el punto anterior. Por lo tanto, también debe existir una bitácora en los cambios de las unidades operativas.

ii. **Persona Autorizada**: Aquí solo se ingresará un número de CUIL que identificará a la persona humana que tendrá el rol de gestor de certificados de aplicaciones. *Esto servirá como identificador para el primer inicio de sesión a la plataforma de gestión de certificados de aplicaciones, ya que el gestor presentará su certificado digital a la aplicación y la misma verificará si el CUIL del certificado se encuentra en la base de datos de gestores de certificados de aplicación.*

4. Luego de seleccionados una persona Autorizante y una persona autorizada, procede a seleccionar la opción de "Otorgar permiso de gestor".

i. Si la asociación ya existe, el sistema informa que la persona Autorizada ya se encuentra asignada como gestor de aplicaciones por esa persona Autorizante.

ii. El sistema registra la asociación mencionada, la marca de tiempo y también el operador que realizó esta acción.

Procedimiento baja:

1. El Responsable de certificados de aplicaciones ingresa al menú de "Administración de gestores de certificados de aplicación" y selecciona la opción para dar de baja un gestor.

2. La aplicación muestra un formulario que permite al usuario ingresar los siguientes datos:

i. Persona Autorizante: Se podrá filtrar por CUIT y por nombre de la organización. El sistema filtrará según lo especificado y permitirá que el usuario seleccione una persona Autorizante.
ii. Persona Autorizada: Se podrá ingresar y filtrar por CUIT de Gestor de certificados de aplicación.

3. El sistema muestra un listado con el/los gestores de certificados de aplicación correspondientes al filtro seleccionado.

4. El usuario selecciona a la derecha del registro de la persona Autorizada la opción para dar de baja.

El sistema registra la acción realizada, con la correspondiente marca de tiempo y datos del operador que realizó esa acción.

b) PASO 1b: ABM de Oficiales de Registro de aplicaciones

Condiciones generales:

- El rol que podrá realizar este proceso será el *RESPONSABLE DE CERTIFICADOS DE APLICACIONES.*

Procedimiento:

1. El Responsable de certificado de aplicación ingresa al menú de "Administración de OR de aplicaciones".

2. Debe poder Listar los OR de aplicaciones existentes; dar de alta uno nuevo y borrar uno existente.

Caso de Alta:

3. Se debe poder Seleccionar un Certificado de Persona humana vigente, para enrolarlo como OR de aplicaciones.

Caso de Baja:

4. Del Listado de OR de aplicaciones existentes; se debe proceder a seleccionar uno para su baja.

c) PASO 2: Gestores de certificados de aplicaciones - Solicitud de certificado.

Condiciones generales:

1. Quien solicita el certificado de aplicación debe poseer un certificado de firma digital y debe estar enrolado como gestor de certificados de aplicación.
2. Debe poseer el request del certificado a solicitar.

3. Se debe establecer en dos años la validez del certificado digital a emitir.

Procedimiento:

4. El usuario ingresa a la pantalla principal de la Aplicación y elije el menú Solicitud de Certificado de aplicación.

5. La aplicación solicita al usuario la presentación de su certificado digital de autenticación y firma.

    - Valida que el certificado digital de autenticación y firma sea válido (*que no esté revocado y que haya sido emitido por una autoridad de certificación autorizada por la AC Raíz*) y vigente; caso contrario se mostrará el error correspondiente.

    - Que el CUIL del certificado se encuentre enrolado como gestor de certificados de aplicación; caso contrario la aplicación le informará que debe ser autorizado según se informa en el procedimiento establecido.

6. Si la aplicación detecta que es la primera vez que inicia de sesión, entonces tomará del certificado el nombre, apellido y correo electrónico (de tenerlo); se los mostrará al usuario dando la posibilidad de "cargar" (en caso de que estuviera vacío) o de "cambiar" la dirección de correo electrónico para continuar y operar con el sistema. En caso de que haya cambiado el mail (diferente al que existe en el certificado) o haya ingresado uno nuevo (porque no había) este deberá ser validado (confirmado) de la misma forma implementada actualmente en el sistema de personas humanas.

    - El usuario podrá, desde el menú de gestión de certificados de aplicación, ver y modificar el correo electrónico de contacto que utilizará para la gestión de los certificados; el cual deberá ser re-validado/confirmado si es modificado para que el cambio sea considerado efectivo.

7. La aplicación muestra la interface de "Gestor de certificados de aplicación", en donde se muestra un listado de la gestión de los certificados de aplicaciones asociados a la unidad operativa informada por la persona autorizante y en la que fue autorizado y vinculado el usuario. El listado contendrá los siguientes datos:

    - Denominación de la aplicación, Fecha de solicitud, Fecha de vencimiento, Estado. Los estados posibles serán:
      Ingreso de solicitud, Confirmación de solicitud, pendiente de evaluación/aprobación, rechazado, emitido, revocado, vencido.

8. El usuario selecciona la opción para tramitar un nuevo certificado de aplicación.

9. La aplicación muestra un formulario para que el usuario complete.

10. El solicitante ingresa el request del certificado (texto) y selecciona la opción de validar.

11. La aplicación valida que el algoritmo de firma utilizado sea SHA2; la longitud de la clave sea de 2048 bits.
    - Si la aplicación no valida los campos mencionados informa al usuario sobre esto y no permite avanzar con el proceso de esa solicitud. Volviendo al paso 4.

12. La aplicación muestra los datos del request para que el solicitante los verifique, agregando los checkbox y combos adicionales que se mencionan más adelante.

13. El solicitante verifica y

    - Marca que acepta que los datos del request ingresados son correctos.

    - Marca que acepta los términos y condiciones

Deben estar todos los campos marcados/seleccionados para habilitar la opción de enviar la solicitud de certificado.

La aplicación debe validar:

    - Que todos los campos han sido marcados/seleccionados.

14. Se guardan los datos del formulario enviado con el estado "Solicitud pendiente de confirmación". También se guarda un registro de auditoría.

15. El sistema genera un identificador de trámite. La aplicación informa por pantalla y envía un correo electrónico al solicitante informando sobre la solicitud ingresada (mostrando todos los datos) y deja un link de confirmación de trámite.

Al final del correo debe decir que si "el" no realizó dicha solicitud, se ponga en contacto de inmediato con los responsables de este servicio.

d) PASO 4: Aprobación de solicitud de certificado.

Condiciones generales:
Esta función estará a cargo del OFICIAL DE REGISTRO DE APLICACIONES. Debe poseer un certificado de firma digital para autenticarse y el permiso correspondiente para ingresar a la aplicación y luego firmar la aprobación.

Procedimiento:

1. El Oficial de Registro de aplicaciones ingresa a la interface de administración de certificados de aplicación y el sistema permite generar un listado de todas las solicitudes de certificados de aplicación, con la posibilidad de filtrar por:

    a. ID de trámite.
    b. Rango de fechas de solicitud.
    c. Estado del trámite.
    d. Denominación de la aplicación (Texto, correspondiente al valor del campo CN del subscriptor).
    e. Organización (Texto) – El texto de búsqueda debe estar contenido en el campo "OrganizationName".
    f. Unidad operativa (Texto) - El texto de búsqueda debe estar contenido en el campo "OrganizationalUnitName".

g. CUIT/CUIL.

2. La aplicación muestra un listado con los siguientes datos:
    a. Fecha de solicitud.
    b. Denominación de la aplicación.
    c. Datos correspondientes al Gestor de certificados de aplicación (Cuit/Cuil, Nombre y apellido, email).
    d. Datos correspondientes a la Entidad y Unidad Operativa relacionadas (datos de CUIT de Entidad y Nombre Unidad Operativa correspondientes a la autorización del Gestor)
    e. *Debe estar ordenado de forma descendente por fecha de solicitud y luego agrupados por Gestor y Unidad Operativa.*

3. Por cada registro en el listado se podrá seleccionar la opción de "ver", la cual permitirá ver el request del certificado, todos los datos ingresados en la solicitud y todos los relacionados con el Gestor.

4. Se podrá aprobar o rechazar (ingresando un detalle) la solicitud, mediante doble confirmación (pop-up que pide confirmar la acción)
    a. Si se acepta la solicitud, el sistema cambia de estado la solicitud a "Solicitud aprobada para su emisión" y la misma es colocada en la cola del sistema para generar el certificado. También se genera un registro de auditoría.

Si se rechaza la solicitud, la misma cambia de estado a "Solicitud rechazada" y envía un email al solicitante informando sobre esto. Se genera un registro de auditoría.

e) PASO 5: Generación de certificado, envío de mail y descarga del certificado.

Procedimiento de generación:

1. Una vez que la CA generó el certificado correspondiente, el sistema cambia el estado de la solicitud a "Emitido".

2. El sistema envía un email al solicitante indicando que el certificado se encuentra listo para su descarga con una URL para que se pueda descargar y el pin de revocación del certificado.

Procedimiento de descarga:

3. El solicitante ingresa a la URL que ha recibido en el correo, lee las instrucciones y descarga el certificado correspondiente.

Asimismo, desde la página web, se debe permitir realizar una búsqueda de los certificados y su estado, requiriendo el ingreso del nombre del dominio y un CAPTCHA complejo. Funcionalidad similar a la que actualmente está implementada en la AC-ONTI de personas humanas.

f) PASO 6: REVOCACIÓN.

El certificado podrá ser revocado:

1. Desde la interface Web, mediante el ingreso del nombre de dominio, PIN de revocación y el CUIT de la Entidad persona Jurídica correspondiente. Se deberá ingresar un motivo y observaciones.

2. Desde la interface de un Gestor de certificados de aplicación. Para esto deberá haber ingresado al sistema y seleccionar para una aplicación en particular la acción de "revocar". Puede ingresar un motivo y observaciones. Esa operación quedará registrada.

3. Desde la interface del Oficial de Registro de aplicaciones. Para esto deberá haber ingresado al sistema y seleccionar para una aplicación en particular la acción de "revocar". Puede ingresar un motivo y observaciones. Esa operación quedará registrada.

Aclaración: el perfil del certificado digital de aplicación debe respetar el definido en la Política de Certificación de la AC ONTI.

ANEXO E

"GENERACIÓN DE CERTIFICADOS PARA SITIOS SEGUROS"

Certificados de Sitio Seguro
Los certificados digitales para sitio seguro permiten a un servidor demostrar su autenticidad y mantener encriptado todo el tráfico de datos entre él y otros equipos.

Arquitectura
La solución encargada debe estar dividida en distintos FrontEnd, uno por Rol. Cada uno de los frontend se deberá construir en .Net Framework, con una arquitectura con separación física de capas mediante servicios WFC. La lógica y validaciones deber encontrarse en un core separado que será el encargado de la persistencia de los datos.

Roles
Se deberá contar con nuevos roles en la aplicación:

- Responsable de Aplicación SSL
- Gestores de certificados SSL
- Oficiales de Registro SSL

Los pasos para la operación serán los siguientes:

a) PASO 1a: ABM de gestores SSL
Condiciones generales:

- El rol que podrá realizar este proceso será el *RESPONSABLE DE APLICACIÓN SSL*. Este rol deberá ser creado en la base de datos de la aplicación.

Procedimiento alta:

1. El responsable de aplicación SSL ingresa al menú de "Administración de gestores SSL".
2. Selecciona la opción para dar de alta un gestor.
3. La aplicación muestra un formulario que le permite ingresar los siguientes datos:

    i. **Persona Autorizante:** Aquí se podrá seleccionar una Unidad Operativa (relacionada a la persona autorizante) precargada en el sistema. Si no existe, se deberá poder lanzar el ABM correspondiente.

- En principio deberá existir:

    i. un ABM de Entidades (Organismos padres) con los siguientes datos para cargar: Nombre de organismo, CUIT.

    ii. un ABM de **personas autorizantes (unidades operativas)** con los siguientes datos para cargar: Seleccionar organismo padre y nombre de la unidad operativa. También se deberá poder indicar si la

designación fue realizada por persona física o persona Jurídica. De ser el caso de persona física el sistema permitirá cargar CUIL, Nombre, Apellido y Mail; en el caso que sea persona Jurídica se deberá poder cargar el nombre de la misma, los datos del Nombre, apellido, CUIL y relación vinculante.

- Es importante destacar que si se actualiza el nombre de una unidad operativa se debe indicar quien hizo la designación como se menciona en el punto anterior. Por lo tanto, también debe existir una bitácora en los cambios de las unidades operativas.

ii. **Persona Autorizada**: aquí solo se ingresará un número de CUIL que identificará a la persona humana que tendrá el rol de gestor SSL. *Esto servirá como identificador para el primer inicio de sesión a la plataforma de gestión SSL, ya que el gestor presentará su certificado digital a la aplicación y la misma verificará si el CUIL del certificado se encuentra en la base de datos de gestores SSL.*

4. Luego de seleccionados una persona Autorizante y una persona autorizada, procede a seleccionar la opción de “Otorgar permiso de gestor SSL”.

   i. Si la asociación ya existe, el sistema informa que la persona Autorizada ya se encuentra asignada como gestor SSL por esa persona Autorizante.

5. El sistema registra la asociación mencionada, la marca de tiempo y también el operador que realizó esta acción.

Procedimiento baja:

6. El Responsable de Aplicación SSL ingresa al menú de “Administración de gestores SSL” y selecciona la opción para dar de baja un gestor.

7. La aplicación muestra un formulario que permite al usuario ingresar los siguientes datos:

   i. Persona Autorizante: Se podrá filtrar por CUIT y por nombre de la organización. El sistema filtrará según lo especificado y permitirá que el usuario seleccione una persona Autorizante.

   ii. Persona Autorizada: Se podrá ingresar y filtrar por CUIT de Gestor SSL

8. El sistema muestra un listado con el/los gestores de SSL correspondientes al filtro seleccionado.

9. El usuario selecciona a la derecha del registro de la persona Autorizada la opción para dar de baja.

10. El sistema registra la acción realizada, con la correspondiente marca de tiempo y datos del operador que realizó esa acción.

b) PASO 1b: ABM de Oficiales de Registro SSL

Condiciones generales:

- El rol que podrá realizar este proceso será el *RESPONSABLE DE APLICACIÓN SSL*.

Procedimiento:

1. El Responsable de Aplicación SSL ingresa al menú de "Administración de OR SSL".
2. Debe poder Listar los OR SSL existentes; dar de alta uno nuevo y borrar uno existente.

Caso de Alta:

3. Se debe poder Seleccionar un Certificado de Persona humana vigente, para Enrolarlo como OR SSL.

Caso de Baja:

4. Del Listado de OR SSL existentes; se debe proceder a seleccionar uno para su baja.

c) PASO 2: Gestores SSL - Solicitud de certificado

Condiciones generales:

1. Quien solicita el certificado SSL debe poseer un certificado de firma digital y debe estar enrolado como gestor de SSL.

2. Debe poseer el request del certificado a solicitar.

3. Se debe establecer en un año la validez del certificado digital a emitir.

Procedimiento:

4. El usuario ingresa a la pantalla principal de la Aplicación y elije el menú Solicitud de Certificado SSL.
5. La aplicación solicita al usuario la presentación de su certificado digital de autenticación y firma.
    a. Valida que el certificado digital de autenticación y firma sea válido (*que no esté revocado y que haya sido emitido por una autoridad de certificación autorizada por la AC Raíz*) y vigente; caso contrario se mostrará el error correspondiente.

    b. Que el CUIL del certificado se encuentre enrolado como gestor de SSL; caso contrario la aplicación le informará que debe ser autorizado según se informa en el procedimiento establecido.

6. Si la aplicación detecta que es la primera vez que inicia de sesión, entonces tomará del certificado el nombre, apellido y correo electrónico (de tenerlo); se los mostrará al usuario dando la posibilidad de "cargar" (en caso de que estuviera vacío) o de "cambiar" la dirección de correo electrónico para continuar y operar con el sistema. En caso de

que haya cambiado el mail (diferente al que existe en el certificado) o haya ingresado uno nuevo (porque no había) este deberá ser validado (confirmado) de la misma forma implementada actualmente en el sistema de personas físicas.

a. El usuario podrá, desde el menú de gestión de SSL, ver y modificar el correo electrónico de contacto que utilizará para la gestión de los certificados; el cual deberá ser re-validado/confirmado si es modificado para que el cambio sea considerado efectivo.

7. La aplicación muestra la interface de "Gestor de SSL", en donde se muestra un listado de la gestión de los certificados SSL asociados a la unidad operativa informada por persona autorizante y en la que fue autorizado y vinculado el usuario. El listado contendrá los siguientes datos:
    a. Dominio, Fecha de solicitud, Fecha de vencimiento, Estado. Los estados posibles serán:
    Ingreso de solicitud, Confirmación de solicitud, validación de control de dominio, pendiente de evaluación/aprobación, rechazado, emitido, revocado, vencido.

8. El usuario selecciona la opción para tramitar un nuevo certificado SSL.

9. La aplicación muestra un formulario para que el usuario complete.

10. El solicitante ingresa el request del certificado (texto) y selecciona la opción de validar.

11. La aplicación valida que el algoritmo de firma utilizado sea SHA2; la longitud de la clave sea de 2048 bits. y que el nombre solicitado NO comience con un "." y no contenga "*"
    a. Si la aplicación no valida los campos mencionados informa al usuario sobre esto y no permite avanzar con el proceso de esa solicitud. Volviendo al paso 4.

12. La aplicación muestra los datos del request para que el solicitante los verifique, agregando los checkbox y combos adicionales que se mencionan más adelante.

13. El solicitante verifica y
    a. Marca que acepta que los datos del request ingresados son correctos.
    b. El solicitante selecciona de un combo, el método de validación a utilizar para demostrar la posesión de dominio:

        i. Validación de posesión de dominio vía correo electrónico.
            1. El usuario podrá seleccionar una de las siguientes cuentas: **webmaster@dominio, postmaster@dominio, hostmaster@dominio**.

        ii. Validación de posesión de dominio con archivo.

Para ambos casos, se muestra el texto de ayuda correspondiente al mecanismo de cada caso seleccionado.

c. Marca que acepta los términos y condiciones

Deben estar todos los campos marcados/seleccionados para habilitar la opción de enviar la solicitud de certificado.

14. La aplicación debe validar:

    a. Que el campo SAN no este vacío.
    b. Que todos los campos han sido marcados/seleccionados.

15. Se guardan los datos del formulario enviado con el estado "Solicitud pendiente de validación". También se guarda un registro de auditoría.

16. El sistema genera un identificador de trámite. La aplicación informa por pantalla y envía un correo electrónico al solicitante informando sobre la solicitud ingresada (mostrando todos los datos) y que diga "Quedamos a la espera del proceso de validación de posesión de dominio solicitado":

    a. Si se eligió la validación por correo electrónico, el mensaje continuará de la siguiente forma: "Usted solicitó el método de validación vía correo electrónico por lo que recibirá un email en la cuenta XXXX (especificada en el punto 10.C) que debe confirmar para poder continuar con el trámite".

    b. Si se eligió la validación con archivo, el mensaje continuará de la siguiente forma: "Usted solicitó el método de validación por archivo por lo que deberá generar un archivo de texto en la dirección **http://dominio/ACONTI_validacionSSL_.txt** y el mismo deberá contener el siguiente código: XXXXXXXXXX….." (Código generado aleatoriamente por la aplicación). Luego deberá contener un link que redirija a la interface de la aplicación para validar la posesión correspondiente.

    c. Al final del correo debe decir que si "el" no realizó dicha solicitud, se ponga en contacto de inmediato con los responsables de este servicio. ***A continuación se explica el proceso de validación en ambos casos.***

PASO 3: Validación de posesión de dominio.

1. **Validación por correo electrónico:** Como se menciona en el punto 13 del apartado anterior, el solicitante recibirá un correo electrónico en la cuenta especificada (webmaster@dominio, postmaster@dominio, hostmaster@dominio) durante la carga del formulario de solicitud SSL. Este correo informará lo siguiente: "Usted debe clickear en el siguiente link para confirmar y continuar con el trámite". El mail deberá tener un link que redirija a una interfaz de la aplicación que le informe al usuario que "Su trámite ha sido confirmado correctamente y se encuentra en espera de evaluación por el Oficial de registro SSL".

2. **Validación con archivo:** Como se menciona en el punto 13 del apartado anterior, el solicitante recibe la información correspondiente sobre la validación de posesión de dominio con archivo a su mail personal especificado.

a. El usuario hace click en el link del correo y el mismo redirige a una interfaz de la aplicación que dice: “A continuación podrá realizar la validación mediante archivo para el dominio XXXX” y donde se detalla además que es lo que se espera validar (la existencia de la url YYYY con el contenido del desafío enviado).
b. La interfaz tendrá un botón que dirá “Validar dominio”.
c. Cuando el usuario hace click en el botón, la aplicación valida que el archivo se encuentre creado y tenga como contenido el código que se generó aleatoriamente y se envió por mail previamente.
    i. *El sistema deberá validar que el tamaño del archivo sea adecuado.*
d. Si la validación es correcta, el sistema muestra al usuario el siguiente mensaje: “Su trámite ha sido confirmado correctamente y se encuentra en espera de evaluación por el Oficial de registro SSL”.
    i. Si la validación es incorrecta, el sistema muestra al usuario el siguiente mensaje: “La posesión no ha podido ser validada porque XXXX” (Debe especificar si no se encontró el archivo o si el contenido del mismo no corresponde con el código generado y enviado)

3. Debe existir la posibilidad para el solicitante de ingresar a una interface de validación de dominio desde el menú de la aplicación. Para esto deberá autenticarse con su certificado de firma digital y tener permiso de gestor SSL.

    a. En esta interfaz, el sistema muestra un listado con todas las solicitudes de certificados de SSL que están asociadas a la unidad operativa del gestor.

    b. A la izquierda del registro de cada solicitud SSL estará la opción de “Validar posesión de dominio”.

    c. Cuando el usuario selecciona la opción mencionada en el punto anterior (b) el sistema muestra la interfaz correspondiente:
        i. Si el método de validación elegido fue por correo electrónico, entonces el sistema muestra el siguiente mensaje “Si usted no ha recibido el correo electrónico correspondiente a su cuenta XXXXXX@dominio haga click en el siguiente botón”. El botón tendrá como texto “Enviar correo de validación”. Cuando el usuario haga click en el botón, el sistema reenviará el correo de confirmación a la cuenta XXXXX@dominio.
        ii. Si el método de validación elegido fue por archivo, entonces el sistema muestra la interfaz mencionada en el punto 2 de este paso.

PASO 4: Aprobación de solicitud de certificado.
Condiciones generales:

1. Esta función estará a cargo del OFICIAL DE REGISTRO SSL. Debe poseer un certificado de firma digital para autenticarse y el permiso correspondiente para ingresar a la aplicación y luego firmar la aprobación.

Procedimiento:

2. El Oficial de Registro SSL ingresa a la interface de administración de certificados

SSL y la aplicación permite generar un listado de todas las solicitudes de certificados SSL, con la posibilidad de filtrar por:

b. ID de trámite.
c. Rango de fechas de solicitud.
d. Estado del trámite. (de la forma que hoy se muestran en la interface de OR para personas físicas)
e. Sitio web (Texto, correspondiente al valor del campo CN del subscriptor).
f. Organización (Texto) – El texto de búsqueda debe estar contenido en el campo "OrganizationName".
g. CUIT/CUIL.
h. IP.
i. DNS.
j. URI.

3. La aplicación muestra un listado con los siguientes datos:

k. Fecha de solicitud.
l. Sitio web.
m. Datos correspondientes al Gestor SSL (Cuit/Cuil, Nombre y apellido, email).
n. Datos correspondientes a la Entidad y Unidad Operativa relacionadas (datos de CUIT de Entidad y Nombre Unidad Operativa correspondientes a la autorización del Gestor)
o. *Debe estar ordenado de forma descendente por fecha de solicitud y luego agrupados por Gestor SSL y Unidad Operativa*

4. Por cada registro en el listado se podrá seleccionar la opción de "ver", la cual permitirá ver el request del certificado, todos los datos ingresados en la solicitud y todos los relacionados con el Gestor

5. Se podrá aprobar o rechazar (ingresando un detalle) la solicitud, mediante doble confirmación (pop-up que pide confirmar la acción)

p. Si se acepta la solicitud, el sistema cambia de estado la solicitud a "Solicitud aprobada para su emisión" y la misma es colocada en la cola del sistema para generar el certificado. También se genera un registro de auditoría.
q. *Si se rechaza la solicitud, la misma cambia de estado a "Solicitud rechazada" y envía un email al solicitante informando sobre esto. Se genera un registro de auditoría.*

PASO 5: Generación de certificado, envío de mail y descarga del certificado.

Procedimiento de generación:

1. Una vez que la CA generó el certificado correspondiente, el sistema cambia el estado de la solicitud a "Emitido".
2. El sistema envía un email al solicitante indicando que el certificado se encuentra listo para su descarga con una URL para que se pueda descargar y el pin de revocación del certificado.

Procedimiento de descarga:

3. El solicitante ingresa a la URL que ha recibido en el correo, lee las instrucciones y descarga el certificado correspondiente.

Asimismo, desde la página web, se debe permitir realizar una búsqueda de los certificados y su estado, requiriendo el ingreso del nombre del dominio y un CAPTCHA complejo. Funcionalidad similar a la que actualmente está implementada en la AC-ONTI de personas humanas.

PASO 6: REVOCACIÓN.

El certificado podrá ser revocado:

1. Desde la interface Web, mediante el ingreso del nombre de dominio, PIN de revocación y el CUIT de la Entidad persona Jurídica correspondiente. Se deberá ingresar un motivo y observaciones.
2. Desde la interface de un Gestor SSL vinculado con ese dominio. Para esto deberá haber ingresado al sistema y seleccionar para un dominio en particular la acción de "revocar". Puede ingresar un motivo y observaciones. Esa operación quedará registrada. Desde la interface del Oficial de Registro SSL. Para esto deberá haber ingresado al sistema y seleccionar para un dominio en particular la acción de "revocar". Puede ingresar un motivo y observaciones. Esa operación quedará registrada.

Aclaración: el perfil del certificado digital de SSL debe respetar el definido en la Política de Certificación de la AC ONTI.

ANEXO F

INTEGRACIÓN CON DATOS BIOMÉTRICOS RENAPER

Se deberán generar nuevas aplicaciones server y cliente para realizar la validación de los datos del RENAPER con datos obtenidos de manera local.

Cada uno de los componentes se deberá construir en .Net Framework, con una arquitectura con separación física de capas mediante servicios WFC. La lógica y validaciones deber encontrarse en un core separado que será el encargado de la persistencia de los datos.

La solución deberá estar compuesta por:

- Módulo de obtención de las huellas dactilares y la fotografía del suscriptor compuesto por:
    - Aplicación cliente: .Net Framework C#, WFC, ClickOnce. Autenticación por firma digital del oficial de registro involucrado. Es la encargada de comunicarse con el lector de huellas dactilares y la cámara conectada al equipo.
    - Aplicación web perimetral: .Net Framework C#, WFC. Realiza la comunicación con la aplicación cliente.
    - Aplicación backend: .Net Framework C#, WFC.
- Modificaciones en las tablas de la base de datos SQL Server para almacenar los datos biométricos capturados y creación de procedimientos almacenados para administrarlos.
- Creación de trazas de auditoría.
- Módulo de verificación de datos integrado a servicios del RENAPER: .Net Framework C#.
- Módulo de verificación fuera de línea en caso de existir problemas de comunicación con los sistemas del RENAPER: .Net Framework C#.
- Configuraciones de networking necesarias para realizar la conexión con los sistemas del RENAPER.
- Será necesario que el sistema permita restringir el acceso por parte de personas o sistemas no autorizados a los datos almacenados.

Anexo 1

FORMULARIO DE LA OFERTA

[El Licitante completará este formulario de acuerdo con las instrucciones indicadas. No se permitirán alteraciones a este formulario ni se aceptarán substituciones.]

Fecha: *[Indicar la fecha (día, mes y año) de la presentación de la oferta]*
SDO No.:**03/2020**

A: *[nombre completo del Comprador]*

Nosotros, los suscritos, declaramos que:

(a) Hemos examinado y no hallamos objeción alguna a los documentos de licitación, incluso sus Enmiendas Nos._____*[indicar el número y la fecha de emisión de cada Enmienda];*

(b) Ofrecemos proveer los siguientes Bienes, Servicios y Servicios Conexos de conformidad con los Documentos de Licitación y de acuerdo con el Plan de Entregas establecido en la Lista de Bienes y Servicios: _____
[indicar una descripción breve de los servicios y servicios conexos];

(c) El precio total de nuestra oferta para los Servicios y Servicios Conexos, excluyendo cualquier descuento ofrecido en el rubro (d) a continuación es: *[indicar el precio total de la oferta en palabras y en cifras, en pesos argentinos, el importe deberá corresponder a la suma de los Formularios de Lista de Servicios y Servicios Conexos];*

(d) Nuestra oferta se mantendrá vigente por el período establecido en la Subcláusula 3.1.2 de la Sección B, a partir de la fecha límite fijada para la presentación de las ofertas de conformidad con la Subcláusula 3.1.1. Esta oferta nos obligará y podrá ser aceptada en cualquier momento antes de la expiración de dicho período;

(e) Si nuestra oferta es aceptada, nos comprometemos a obtener una Garantía de Cumplimiento del Contrato de conformidad con la Subcláusula 3.14 de la Sección B;

(f) Los suscritos, incluyendo todos los subcontratistas o proveedores requeridos para ejecutar cualquier parte del Contrato, tenemos nacionalidad de países elegibles_____*[indicar la nacionalidad del Licitante, incluso la de todos los miembros que comprende el Licitante, si el Licitante es una*

Asociación en Participación o Consorcio, y la nacionalidad de cada subcontratista y proveedor]

(g) No tenemos conflicto de intereses de conformidad con la Subcláusula 1.5.2 de la Sección A;

(h) Nuestra empresa, sus afiliados o subsidiarias, incluyendo todos los subcontratistas o proveedores para ejecutar cualquier parte del Contrato, no han sido declarados inelegibles por el Banco, bajo las leyes del país del Comprador o normativas oficiales, de conformidad con la Subcláusula 1.5.3 de la Sección A;

(i) Entendemos que esta oferta, junto con su debida aceptación por escrito, incluida en la notificación de adjudicación, constituirán una obligación contractual entre nosotros, hasta que el Contrato formal haya sido perfeccionado por las partes.

(j) Entendemos que ustedes no están obligados a aceptar la oferta evaluada más baja ni ninguna otra oferta que reciban.

Firma:_____*[indicar el nombre completo de la persona cuyo nombre y calidad se indican]*
En calidad de_____*[indicar la capacidad jurídica de la persona que firma el Formulario de la Oferta]*

Nombre:_____*[indicar el nombre completo de la persona que firma el Formulario de la Oferta]*

Debidamente autorizado para firmar la oferta por y en nombre de:
[*indicar el nombre completo del Licitante]*

El día_____del mes_____del año _____
[indicar la fecha de la firma]

Anexo 2

LISTA DE PRECIOS

Fecha:

SDO No:_____ Página N° ___de _____

1	2	3	4	5	6
No. LOTE/ITEM	DESCRIPCION DE LOS BIENES Y SERVICIOS	PLAZO DE ENTREGA	PRECIO DEL SERVICIO SIN IMPUESTOS	IMPUESTOS	PRECIO TOTAL SERVICIO CON IMPUESTOS INCLUIDOS
[indicar No. de Lote/Item]	*[indicar nombre de los servicios]]*	*[indicar la fecha de entrega ofertada]*	*[indicar precio del servicio sin impuestos]*	*[Indicar el monto correspondiente a los impuestos]*	*[Indicar el precio total de los servicios con impuestos]*
			Precio Total		

Nombre del Licitante *[indicar el nombre completo del Licitante]* Firma del Licitante *[~~firma de la persona que firma la oferta~~]* Fecha *[Indicar Fecha]*

Anexo 3
FORMULARIO DE SERVICIOS CONEXOS

Precio y Cronograma de Cumplimiento - Servicios Conexos

Fecha:_____
SDO No: _____
Página N° de

1	2	3	4	5	6
Servicio N °	Descripción de los Servicios	Fecha de Entrega en el Lugar de Destino Final	Cantidad y Unidad física	Precio Mensual con impuestos	Precio Total por Servicio con impuestos incluidos (Col 4 x 5)
[indicar número del servicio]	*[indicar el nombre de los Servicios]*	*[indicar la fecha de entrega al lugar de destino final por servicio]*	*[indicar le número de unidades a suministrar y el nombre de la unidad física de medida]*	*[indicar el precio unitario por servicio]*	*[indicar el precio total por servicio]*
			Precio Total de los servicios conexos		

Nombre del Licitante *[indicar el nombre completo del Licitante]* Firma del Licitante *[firma de la persona que firma la oferta]* Fecha *[Indicar Fecha]*

Anexo 4
MANIFIESTO DE GARANTIA DE LA OFERTA

[El Licitante completará este Formulario de Manifiesto de Garantía de la Oferta de acuerdo con las instrucciones indicadas.]

Fecha: *[indicar la fecha (día, mes y año) de presentación de la oferta]*

SDO No.: *[indicar el número del proceso licitatorio]*

A: Dirección de Gestión Programas y Proyectos

Nosotros, los suscritos, declaramos que:

1. Entendemos que, de acuerdo con sus condiciones, las ofertas deberán estar respaldadas por un Manifiesto de Garantía de la Oferta.

2. Aceptamos que automáticamente seremos declarados inelegibles para participar en cualquier licitación de contrato con el Comprador por un período de 2 años contado a partir de a partir de la apertura de la licitación si violamos nuestra(s) obligación(es) bajo las condiciones de la oferta si:

(a) retiráramos nuestra Oferta durante el período de vigencia de la oferta especificado por nosotros en el Formulario de Oferta; y/o

(b) no aceptáramos las correcciones aritméticas realizadas por el Comprador; y/o

(c) si después de haber sido notificados de la aceptación de nuestra Oferta durante el período de validez de la misma, (i) no ejecutamos o rehusamos ejecutar el formulario del Convenio de Contrato, si es requerido; o (ii) no suministramos o rehusamos suministrar la Garantía de Cumplimiento de conformidad con las instrucciones de la carta de invitación.

3. Entendemos que este Manifiesto de Garantía de la Oferta expirará si no somos los seleccionados, y cuando ocurra el primero de los siguientes hechos: (i) si recibimos una copia de su comunicación con el nombre del Licitante seleccionado; o (ii) han transcurrido veintiocho días después de la expiración de nuestra Oferta.

Firmada: *[insertar la firma de la persona cuyo nombre y capacidad se indican]*.
En capacidad de *[indicar la capacidad jurídica de la persona que firma el Manifiesto de Garantía de la Oferta]*

Nombre: *[indicar el nombre completo de la persona que firma el Manifiesto de Garantía de la Oferta]*

Debidamente autorizado para firmar la oferta por y en nombre de: *[indicar el nombre completo del Licitante]*

Fechada el _____ día de _____ de 2020
[indicar la fecha de la firma]

Anexo 5
LISTA DE SERVICIOS Y PLAN DE ENTREGAS

N° de LOTE	Descripción de los Servicios/Bienes	Lugar de Entrega	Fecha de Entrega	
			Fecha Límite de Entrega desde la firma del contrato	Fecha de Entrega Ofrecida por el Licitante[10]
UNICO	1.1.Equipamiento 1.1.1 4 (cuatro)Switches de Red 1.1.2 10 (diez) Servidores de Red 1.1.3 8 (ocho) Firewall)	Sala cofre de la AFIP, Hipólito -Irigoyen 370-CABA	30 días	
	1.2.Actualización funcional de la Plataforma para nuevas prestaciones	Sala cofre de la AFIP, Hipólito -Irigoyen 370-CABA	120 días	
	1.3 Migración de la Plataforma actualizada a la nueva infraestructura	Sala cofre de la AFIP, Hipólito -Irigoyen 370-CABA	210 días	
SERVICIOS CONEXOS	1.4 Capacitación (4 cursos)	A determinar por el comprador	30 días (*)	
	1.5 Soporte Técnico integral	Sala cofre de la AFIP, Hipólito -Irigoyen 370-CABA	Anual (**)	

(*) Este plazo se cuenta una vez finalizada la entrega de todos los ítems anteriores.
(**) Este plazo rige a partir de la puesta en operación de la Plataforma y el Equipamiento.

[10] No se admiten plazos superiores a los máximos establecidos.

Anexo 6
AUTORIZACIÓN DEL FABRICANTE/DISTRIBUIDOR

[El Licitante solicitará al Fabricante que complete este formulario de acuerdo con las instrucciones indicadas. Esta carta de autorización deberá estar escrita en papel membrete del Fabricante y deberá estar firmado por la persona debidamente autorizada para firmar documentos que comprometan el Fabricante. El Licitante lo deberá incluir en su oferta, si así ***se establece en la Subcláusula 3.4.1 de la Sección B****.]*

Fecha: *[indicar la fecha (día, mes y año) de presentación de la oferta]*
SDO No.: *[indicar el número del proceso licitatorio]*

A: *[indicar el nombre completo del Comprador]*

POR CUANTO

Nosotros *[indicar nombre completo del Fabricante]*, como fabricantes oficiales de *[indique el nombre de los bienes fabricados]*, con fábricas ubicadas en *[indique la dirección completa de las fábricas]* mediante el presente instrumento autorizamos a *[indicar el nombre completo del Licitante]* a presentar una oferta con el solo propósito de suministrar los siguientes Bienes de fabricación nuestra *[nombre y breve descripción de los bienes]*, y a posteriormente negociar y firmar el Contrato.

Por este medio extendemos nuestro aval y plena garantía, conforme a la Subcláusula 4.1.1 de la Sección D, respecto a los bienes ofrecidos por la firma antes mencionada.

Firma: _____
[indicar firma del(los) representante(s) autorizado(s) del Fabricante]

Nombre: *[indicar el nombre completo del representante autorizado del Fabricante]*

Cargo: *[indicar cargo]*

Debidamente autorizado para firmar esta Autorización en nombre de: *[nombre completo del Licitante]*

Fechado en el día_____de_____de___*[fecha de la firma]*

Anexo 7
FORMULARIO DE CONTRATO

[El Licitante seleccionado completará este formulario de acuerdo con las instrucciones indicadas]

ESTE CONVENIO DE CONTRATO es celebrado

El día *[indicar: **número**]* de *[indicar: **mes**]* de *[indicar: **año**]*.

ENTRE

(1) *[indicar nombre completo del Comprador]*, una *[indicar la descripción de la entidad jurídica, por ejemplo, una Agencia del Ministerio de .... del Gobierno de {indicar el nombre del país del Comprador}, o corporación integrada bajo las leyes de {indicar el nombre del país del Comprador}]* y físicamente ubicada en *[indicar la dirección del Comprador]* (en adelante denominado "el Comprador"), y

(2) *[indicar el nombre del Proveedor]*, una corporación incorporada bajo las leyes de *[indicar: nombre del país del Proveedor]* físicamente ubicada en *[indicar: dirección del Proveedor]* (en adelante denominada "el Proveedor").

POR CUANTO el Comprador ha llamado a licitación respecto de ciertos Servicios, *[inserte una breve descripción de los servicios]* y ha aceptado una oferta del Proveedor para el suministro de dichos Servicios por la suma de *[indicar el Precio del Contrato en palabras y cifras expresado en la(s) moneda(s) del Contrato y]* (en adelante denominado "Precio del Contrato"), el cual se conforma de acuerdo al siguiente detalle:

Lote	Descripción	Cant.	Monto Total sin impuestos	Impuestos	Monto Total con impuestos	Plazo de entrega

ESTE CONVENIO ATESTIGUA LO SIGUIENTE:

1. En este Convenio las palabras y expresiones tendrán el mismo significado que se les asigne en las respectivas condiciones del Contrato a que se refieran.

2. Los siguientes documentos constituyen el Contrato entre el Comprador y el Proveedor y, por lo tanto, serán leídos e interpretados como parte integrante del mismo:
   (a) Este Contrato;
   (b) Las Condiciones Contractuales;
   (c) La oferta del Proveedor y las Listas de Precios originales;
   (d) Los Requerimientos Técnicos (incluyendo la Lista de Requisitos y las Especificaciones Técnicas);
   (e) La notificación de intención de Adjudicación del Contrato emitida por el Comprador.

3. Este Contrato prevalecerá sobre todos los otros documentos contractuales. En caso de alguna discrepancia o inconsistencia entre los documentos del Contrato, los documentos prevalecerán en el orden enunciado anteriormente.

4. En consideración a los pagos que el Comprador hará al Proveedor conforme a lo estipulado en este Contrato, el Proveedor se compromete a proveer los Servicios al Comprador y a subsanar los defectos de éstos; ello, de conformidad con las disposiciones del Contrato correspondientes.

5. El Comprador se compromete a pagar al Proveedor, como contrapartida del suministro de los servicios y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en el Contrato en el plazo y en la forma prescritos en éste.

EN TESTIMONIO de lo cual las partes han ejecutado el presente Convenio de conformidad con las leyes de *[indicar el nombre de la ley del país que gobierna el Contrato]* en el día, mes y año antes indicados.

Por y en nombre del Comprador

Firmado: *[indicar firma]*
en capacidad de *[indicar el título u otra designación apropiada]*
en la presencia de *[indicar la identificación del testigo]*

Por y en nombre del Proveedor

Firmado: *[indicar la(s) firma(s) del (los) representante(s) autorizado(s) del Proveedor]*
en capacidad de *[indicar el título u otra designación apropiada]*
en la presencia de *[indicar la identificación del testigo]*

Anexo 8
GARANTÍA DE CONTRATO
Póliza de Seguro de Caución

PÓLIZA Nº [*indicar el **número***]

CONDICIONES PARTICULARES

Esta Compañía [*indicar el **nombre de la Compañía Aseguradora***], EL ASEGURADOR, con domicilio en [*indicar el **domicilio***], en su carácter de fiador solidario, con renuncia a los beneficios de excusión y división y con arreglo a las Condiciones Generales[11] que forman parte de esta póliza y a las Particulares que seguidamente se detallan, asegura a: [*indicar el **Nombre del Comprador***], EL ASEGURADO, con domicilio en [*indicar el **Domicilio del Comprador***] el pago de hasta la suma de [*indicar **la moneda y el monto***] que resulte adeudarle [*indicar **el nombre del Licitante***] EL TOMADOR, con domicilio en [*indicar el **domicilio del Licitante***] por afectación de la garantía que de acuerdo a la ley, las bases de licitación y el contrato, en su caso, está obligado a constituir según el objeto que se indica en las Condiciones Generales integrantes de esta póliza.

OBJETO DE LA LICITACIÓN
Licitación [***indicar nombre y número del Llamado a Licitación***]
Contrato [***indicar nombre y número del Contrato***]
Préstamo/Crédito Nº: [***indicar: número del préstamo o crédito***]

El presente seguro regirá desde la 0 hora del día [***indicar la fecha de la oferta***] hasta la extinción de las obligaciones del TOMADOR cuyo cumplimiento cubre.
Las cláusulas y anexos que seguidamente se detallan, firmadas y adheridas a las Condiciones Particulares, forman parte integrante de la presente póliza.

A los fines que hubiere lugar, EL ASEGURADOR, fija domicilio en: [***indicar el domicilio***]

Fecha: [***indicar fecha de emisión de la póliza***]
Por y en nombre de la Compañía Aseguradora:

_____ _____

(Firma) *(Firma)*

[11]Deberá adjuntarse la transcripción de las condiciones generales tipo aplicables a las pólizas de seguro de caución.

_____ _____

_____
(Nombre y cargo) *(Nombre y cargo)*

Fecha: _____
en calidad de: *[indicar:* ***cargo u otra designación apropiada****]*
Sello de la Compañía Aseguradora

"Esta póliza ha sido aprobada por la Superintendencia de Seguros de la Nación (Resolución Nº….)."

República Argentina - Poder Ejecutivo Nacional
2020 - Año del General Manuel Belgrano

Hoja Adicional de Firmas
Pliego

Número: PLIEG-2020-57110979-APN-SSGAIP#JGM

CIUDAD DE BUENOS AIRES
Viernes 28 de Agosto de 2020

Referencia: Pliego SDO

El documento fue importado por el sistema GEDO con un total de 83 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2020.08.28 15:24:47 -03:00

Maria Soledad Segovia
Asesor Legal
Subsecretaría de Gestión Administrativa de Innovación Pública
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2020.08.28 15:24:48 -03:00