

**DECRETOS****G O B I E R N O D E L A P R O V I N C I A D E B U E N O S A I R E S****Decreto**

**Número:** DECTO-2017-944-E-GDEBA-GPBA

LA PLATA, BUENOS AIRES  
Miércoles 27 de Diciembre de 2017

**Referencia:** Corresponde Expediente N° 2319-24461/2016

---

**VISTO** el expediente N° 2319-24461/2016 y agregado mediante el cual el Instituto Provincial de Lotería y Casinos propicia el llamado a Licitación Pública tendiente a contratar la provisión y mantenimiento de Máquinas Electrónicas de Juegos de Azar Automatizadas, el Control On Line de las mismas, la remodelación, construcción y/o cesión y puesta en valor de las distintas Salas de Juego y una variedad de Servicios Complementarios y anexos a la actividad lúdica, y

**CONSIDERANDO:**

Que por Resolución N° 711/16 la Contaduría General de la Provincia, en su carácter de Autoridad de Aplicación, aprobó el Pliego de Bases y Condiciones Generales para la contratación de Bienes y Servicios, el cual es de uso obligatorio para todos los procesos de contratación, sin modificación alguna y bajo pena de nulidad;

Que el Instituto Provincial de Lotería y Casinos de la Provincia de Buenos Aires, propicia la autorización del llamado a Licitación Pública y la aprobación del Pliego de Bases y Condiciones Particulares y Especificaciones Técnicas tendientes a la provisión y mantenimiento de Máquinas Electrónicas de Juegos de Azar Automatizadas, el Control On Line de las mismas, la remodelación, construcción y/o cesión, y puesta en valor de las distintas Salas de Juego y una variedad de Servicios Complementarios y anexos a la actividad lúdica en los Casinos de Tigre, Pinamar, Tandil, Miramar, Hermitage, Central y Monte Hermoso, por un término de veinte (20) años con opción a prórroga por un (1) año adicional;

Que la Dirección Provincial de Administración y Finanzas del Instituto Provincial ha elaborado el Pliego de Bases y Condiciones Particulares y Especificaciones Técnicas, las cuales regirán el llamado a Licitación Pública;

Que la fijación del lugar, día y hora para la apertura de ofertas del presente certamen será delegada en el titular de la autoridad administrativa del Instituto, conforme lo previsto en el artículo 14 apartado 2 inciso e) del Anexo I del Decreto N° 1.300/16;

Que el llamado de referencia se encuadra en las previsiones del artículo 17 de la Ley N° 13.981 y en el artículo 17 apartado 1 -Licitación Pública- y apartado 2 -de Etapa Múltiple- del Anexo I del mencionado Decreto Reglamentario;

Que se han expedido favorablemente la Dirección Provincial de Administración y Finanzas a fojas 180/186 vuelta y la Dirección Jurídico Legal a fojas 443/444, ambas dependientes del Instituto Provincial de Lotería y Casinos;

Que emitieron opinión la Dirección Provincial de Sistemas de Información y Tecnologías a fojas 458/459, la Dirección de Ingeniería del Ministerio de Jefatura de Gabinete de Ministros a fojas 460, y la Dirección Provincial de Operaciones y Tecnologías del Capital Humano del Ministerio de Economía a fojas 463/465;

Que el Presidente del Instituto Provincial de Lotería y Casinos, presta conformidad con la presente gestión a fojas 665/666;

Que conforme lo previsto por el artículo 20 apartado 2) del Anexo I del Decreto N° 1300/16, la Comisión de Preadjudicación que intervendrá en la presente Licitación Pública, estará integrada por Sabrina Wolff, DNI 33.899.517; Laura Virginia Costancio, DNI 28.723.822, Sabrina Minin DNI 28.171.022;

Que han tomado la intervención de su competencia Asesoría General de Gobierno a fojas 451/453, Contaduría General de la Provincia a fojas 455/456 y Fiscalía de Estado a fojas 448/450;

Que la presente se dicta de conformidad con lo establecido en el Anexo II del Decreto N° 1300/16 y en uso de las facultades conferidas por el Artículo 144 -proemio- de la Constitución de la Provincia de Buenos Aires;

Por ello,

## LA GOBERNADORA DE LA PROVINCIA DE BUENOS AIRES

### DECRETA

**ARTÍCULO 1º.** Autorizar el llamado a Licitación Pública para la contratación de un servicio integral para los Casinos Oficiales Central de Mar del Plata, Casino Anexo III de Mar del Plata (Hotel Hermitage), Casino de Miramar, Casino de Monte Hermoso, Casino de Pinamar, Casino de Tigre y Casino de Tandil, por un período de veinte (20) años contados a partir de la fecha de suscripción del contrato, con posibilidad de prórroga de un (1) año adicional a opción del Instituto, con encuadre en lo establecido en los artículos 7 inciso f) y 17 de la Ley N° 13.981 y en el artículo 17 apartado 1 -Licitación Pública- y apartado 2 -de Etapa Múltiple- del Anexo I del Decreto Reglamentario N° 1.300/16.

**ARTÍCULO 2º.** Aprobar el Pliego de Bases y Condiciones Particulares y Especificaciones Técnicas, contenidos en el documento GEDO N° PLIEG-2017-05863125-GDEBA-DJLIPLYC, que regirán el llamado a Licitación Pública y que forman parte integrante del presente Decreto, los cuales podrán ser consultados en el sitio web [www.gba.gob.ar/contrataciones](http://www.gba.gob.ar/contrataciones).

**ARTÍCULO 3º.** Fijar el precio del Pliego de Bases y Condiciones en la suma de pesos Quinientos mil (\$500.000.-) el que podrá ser abonado a través de la boleta de pago obtenida en la Guía Única de Trámites ([www.gba.gov.ar](http://www.gba.gov.ar)) o mediante depósito en la Cuenta Fiscal N° 229/7 - del Banco de la Provincia de Buenos Aires, orden Tesorero General de la Provincia o Contador General de la Provincia, en concepto de “Adquisición Pliego de Bases y Condiciones -Licitación Pública - Expediente N° 2319-24461/16 y agregado”.

**ARTÍCULO 4º.** Delegar en el funcionario titular de la autoridad administrativa del organismo licitante, la fijación del lugar, día y hora de apertura de ofertas.

**ARTÍCULO 5º.** Establecer que conforme lo normado por el artículo 20 apartado 2) del Anexo I del Decreto N° 1300/16, la Comisión de Preadjudicación que intervendrá en la presente Licitación Pública, estará integrada por Sabrina Wolff, DNI 33.899.517; Laura Virginia Costancio, DNI 28.723.822, Sabrina Minin DNI 28.171.022.

**ARTÍCULO 6º.** Autorizar al Instituto Provincial de Lotería y Casinos a gestionar la publicación en el Boletín Oficial y simultáneamente en el sitio Web de la Provincia de Buenos Aires, de conformidad con lo estipulado en el Artículo 15 del Anexo I del Decreto N° 1300/16, reglamentario de la Ley N° 13981.

**ARTÍCULO 7º.** El presente Decreto será refrendado por el Ministro Secretario en el Departamento de Jefatura de Gabinete de Ministros

**ARTÍCULO 8º.** Registrar, notificar al Fiscal de Estado, comunicar, publicar, dar al Boletín Oficial y al SINBA. Cumplido, archivar.

Digitally signed by SALVAI Carlos Federico  
Date: 2017.12.27 10:15:07 ART  
Location: Provincia de Buenos Aires

Federico Salvai  
Ministro  
Ministerio de Jefatura de Gabinete de Ministros

Digitally signed by VIDAL María Eugenia  
Date: 2017.12.27 20:31:44 ART  
Location: Provincia de Buenos Aires

María Eugenia Vidal  
Gobernadora  
Gobierno de la Provincia de Buenos Aires

Digitally signed by GDE BUENOS AIRES  
DN: cn=GDE BUENOS AIRES, c=AR, o=MINISTERIO DE  
JEFATURA DE GABINETE DE MINISTROS BS AS,  
ou=SUBSECRETARIA para la MODERNIZACION DEL  
ESTADO, serialNumber=CUIT 30715471511  
Date: 2017.12.27 20:32:55 -03'00'



## CAPÍTULO I

### **PLIEGO DE BASES Y CONDICIONES GENERALES PARA LA CONTRATACION DE BIENES Y SERVICIOS**

#### **ARTÍCULO 1º.- ÁMBITO DE APLICACIÓN**

Las normas contenidas en el presente articulado, constituyen el PLIEGO DE BASES Y CONDICIONES GENERALES PARA LA CONTRATACIÓN DE BIENES Y SERVICIOS aplicable a todos los procedimientos reglamentados y contratos estipulados en el Decreto N° 1.300/16.

#### **ARTÍCULO 2º.- ADQUISICIÓN DE LOS PLIEGOS DE BASES Y CONDICIONES.**

Los Pliegos de Bases y Condiciones se suministrarán en forma gratuita en el sitio de internet de la Contaduría General de la Provincia de Buenos Aires ([www.gba.gov.ar](http://www.gba.gov.ar)).

Sin perjuicio de ello, en aquellos casos en que fundadamente y por sus características el organismo contratante determine que para ofertar sea requerido el pago de una suma para la adquisición del Pliego de Bases y Condiciones Particulares, ésta será establecida en la convocatoria, y no podrá superar el medio por ciento (0,50%) del monto estimado de la contratación.

En este último caso, sólo se tendrán en cuenta las ofertas presentadas por las firmas que hayan abonado, previo a la apertura de ofertas, el arancel correspondiente al valor del pliego.



El importe recibido por la venta de pliegos no será devuelto a los adquirentes en ningún caso.

### **ARTÍCULO 3º.-COMUNICACIONES**

Las comunicaciones que se realicen entre el contratante y los interesados, oferentes, preadjudicatarios y adjudicatarios, serán efectuadas al domicilio electrónico dispuesto por el artículo 12 del Decreto Reglamentario N° 1.300/16.

### **ARTÍCULO 4º.- DOCUMENTACIÓN A INTEGRAR EN LA OFERTA**

Los interesados en formular ofertas deberán:

1) Acreditar su inscripción en el Registro de Proveedores y Licitadores acompañando el número correspondiente; o haber dado inicio al trámite mediante la presentación del formulario de inscripción, el que tendrá carácter de declaración jurada. En el último caso, el oferente deberá, bajo pena de tener por desistida la oferta, con pérdida de la garantía, encontrarse inscripto como proveedor, mediante el número correspondiente, en forma previa a la preadjudicación o, si se trata de un procedimiento de etapa múltiple, a la preselección.

En caso de que la preadjudicación o preselección corresponda a una Unión Transitoria a constituirse, con carácter previo a la adjudicación y bajo pena de tener por desistida la oferta, con pérdida de la garantía, deberá acreditarse la inscripción en el Registro de Proveedores y Licitadores como Unión Transitoria constituida.

Sólo podrán ser admitidas y adjudicadas ofertas de proponentes no inscriptos en los supuestos previstos en el apartado 3.1 del artículo 11 del Anexo I del Decreto N° 1.300/16.

2) Cumplir con las siguientes obligaciones:



- a) Presentar el Formulario A-404 aprobado por la Resolución Normativa 50/2011 (artículo 37, Ley N° 11.904), de la Agencia de Recaudación de la Provincia de Buenos Aires.
- b) Presentar el Certificado Fiscal para contratar emitido por la Administración Federal de Ingresos Públicos (AFIP).
- c) Presentar la totalidad de la documentación legal y contable que exija el Pliego de Condiciones Particulares.

#### **ARTÍCULO 5°.- CONSTITUCIÓN DE DOMICILIOS**

Todo oferente deberá indicar su domicilio real, legal y electrónico.

El domicilio legal deberá ser fijado en la Provincia de Buenos Aires, y el electrónico, onstituido conforme a las normas que dicte la Autoridad de Aplicación en la especie.

Serán válidas todas las notificaciones electrónicas que sean cursadas por el contratante en el domicilio electrónico constituido.

La falta de constitución del domicilio electrónico configurará un requisito no subsanable en caso de proponentes que no tengan la obligación de estar inscriptos en el Registro de Proveedores y Licitadores para ser preadjudicados, conforme apartado 3.I del artículo 11 del Anexo I, del Decreto N° 1.300/16.

Todo cambio de domicilio deberá ser comunicado fehacientemente al contratante y surtirá efecto una vez transcurridos diez (10) días de su notificación.

#### **ARTÍCULO 6°.- COMPETENCIA JUDICIAL:**

Toda cuestión judicial que se suscite en torno a los procedimientos de selección previstos en la Ley N° 13.981, normas reglamentarias y complementarias, así como



a los contratos que se perfeccionen bajo su vigencia, quedarán sometidas única y expresamente a la jurisdicción de los Tribunales Contenciosos Administrativos de la Provincia de Buenos Aires

#### **ARTÍCULO 7°.- CÓMPUTO DE PLAZOS**

Los plazos deben computarse en días hábiles administrativos, salvo disposición expresa en contrario.

#### **ARTÍCULO 8°.- CONDICIÓN FRENTE AL I.V.A.**

A los efectos emergentes del Impuesto al Valor Agregado (I.V.A.), la Provincia de Buenos Aires reviste la condición de exento; en consecuencia, en las propuestas económicas que el interesado presente junto a las ofertas no se deberá discriminar el importe correspondiente a la incidencia de este impuesto, debiendo incluirse el mismo en el precio cotizado.

Las jurisdicciones y entidades alcanzadas por esta norma cuya condición no se corresponda con lo citado en los párrafos anteriores deberán consignar los datos que les son propios.

#### **ARTÍCULO 9°.- DECLARACIÓN JURADA DE APTITUD PARA CONTRATAR**

El oferente deberá presentar una declaración jurada que manifieste la inexistencia de las causales de inhabilidad previstas en el art. 16, apartado III del Decreto N° 1.300/16.

La Comisión de Preadjudicación podrá verificar la veracidad de los datos en cualquier etapa del procedimiento.



La falsedad de los datos así como también de la documentación acompañada implicará la pérdida de las garantías y la suspensión del oferente en el Registro de Proveedores y Licitadores por el plazo máximo previsto en reglamentación de la Ley N° 13.981.

Si la falsedad fuera detectada durante el plazo de cumplimiento del contrato hará pasible al adjudicatario de la aplicación de la sanción de rescisión del contrato.

#### **ARTÍCULO 10: PRESENTACIÓN DE LAS OFERTAS**

Las ofertas serán presentadas por duplicado y deberán estar firmadas por el oferente o su representante legal. La firma deberá encontrarse aclarada indicando el carácter del firmante.

Las ofertas deberán encontrarse firmadas en todas sus fojas, incluyendo aquellas que expresamente requiera el Pliego de Bases y Condiciones Particulares, más la documentación adicional, folletos o todo tipo de publicidad que el oferente adjunte y foliadas en forma correlativa.

#### **ARTÍCULO 11.- MONEDA DE COTIZACIÓN**

La moneda de cotización será el Peso (\$), excepto que las condiciones particulares prevean la posibilidad de cotizar en moneda extranjera.

Cuando el llamado se efectúe en moneda extranjera:

- 1) El importe de las garantías se calculará en base al tipo de cambio al cierre del día anterior al que se extienda, según el tipo de cambio vendedor del Banco Nación.
- 2) A los efectos de la comparación de precios, se convertirá en base al tipo de cambio vendedor, vigente en el Banco de la Nación Argentina al día anterior al de la apertura de sobres.



## **ARTÍCULO 12. APERTURA**

Las propuestas se abrirán en el lugar, día y hora indicados en el pliego de condiciones particulares, en presencia de las autoridades de la repartición contratante y de todos aquellos que decidan presenciarlo.

Si el día fijado para ese acto fuere feriado o declarado asueto administrativo éste tendrá lugar el primer día hábil siguiente a la misma hora.

En los procedimientos de etapa múltiple, la recepción de los sobres debe ser simultánea para todas las ofertas, en la fecha y hora fijada para la apertura del sobre número uno. El sobre correspondiente a la oferta económica sólo se abrirá si el oferente fuere seleccionado en las etapas previas; caso contrario, se procederá a la devolución de los sobres sin abrir.

## **ARTÍCULO 13.- MANTENIMIENTO DE LA OFERTA**

Los oferentes deberán mantener y garantizar los términos de su oferta por el término de veinte (20) días, o el que se fije en los Pliegos de Bases y Condiciones Particulares, a contar de la fecha de la apertura. Si el oferente no manifestara en forma fehaciente su voluntad de no renovar la garantía de mantenimiento de oferta con una antelación mínima de diez (10) días anteriores al vencimiento del plazo, aquélla se considerará prorrogada automáticamente por un lapso igual al inicial, salvo que el Pliego disponga otro distinto.

## **ARTÍCULO 14.- EFECTOS DE LA PRESENTACIÓN DE LA OFERTA**



La presentación de la oferta implica el sometimiento voluntario y sin reservas a las disposiciones de la Ley N° 13.981, al Decreto N° 1.300/16 y a las Bases y Condiciones de la contratación, sus Especificaciones Técnicas y circulares dictadas de oficio o como respuesta a consulta.

No será necesaria la presentación de los Pliegos de Bases y Condiciones con la oferta, salvo que éstos sean solicitados como requisito junto con la documentación que la integra.

#### **ARTÍCULO 15. OFERTAS- ELEMENTOS A IMPORTAR**

Cuando se hubiere previsto la oferta de elementos a importar, la autorización a cotizar en moneda extranjera puede referirse al país de origen de los bienes u otras monedas usuales en el comercio internacional y según condición de INCOTERMS prevista en el pliego.

En caso de que el pliego nada diga en este último aspecto, se entiende que la oferta ha sido requerida en condición C.I.F., Puerto de Buenos Aires.

Los seguros para las ofertas en condición C.I.F., deben siempre cotizarse separadamente del valor de la mercadería. Esta cláusula se toma en cuenta para la comparación de precios y cómputo de los beneficios por aplicación de los principios de prioridad de contratación, incluyendo también aranceles y derechos de nacionalización y todo otro gravamen que corresponda hasta la efectiva entrega.

La gestión para obtener la liberación de recargos, derechos aduaneros y otros gravámenes correspondientes al elemento adjudicado, está a cargo de la Autoridad Administrativa y debe ser tramitada y obtenida antes de la apertura de la carta de crédito, entendiéndose que si el beneficio previsto no pudiera obtenerse por aspectos no considerados, el contrato puede ser rescindido sin responsabilidad alguna.



## **ARTÍCULO 16. OFERTAS- PREFERENCIAS**

Cuando se pretenda la aplicación de las preferencias previstas por el artículo 22 de la Ley N° 13.981, en forma conjunta con la oferta, deberá presentarse la documentación que acredite los extremos legales.

## **ARTÍCULO 17. FALSEAMIENTO DE DATOS**

El falseamiento de datos contenidos en la oferta dará lugar a la inmediata exclusión del oferente, sin lugar a la devolución de la garantía de mantenimiento que se hubiere constituido.

Si la falsedad fuere advertida con posterioridad a la contratación, será causal de rescisión por culpa del contratista, con pérdida de la garantía de cumplimiento del contrato, y sin perjuicio de las demás responsabilidades que pudieren corresponder.

## **ARTÍCULO 18.- COTIZACIONES PARCIALES**

El oferente debe formular oferta por la totalidad de los bienes y/o servicios solicitados para cada renglón, salvo que los pliegos en sus Cláusulas Particulares admitan cotizaciones por parte del renglón.

## **ARTÍCULO 19.- GARANTÍAS**

Para afianzar el cumplimiento de todas sus obligaciones los interesados, oferentes y adjudicatarios deberán constituir garantías conforme dispone el artículo 19 del Anexo I del Decreto N° 1.300/16 y los Pliegos Particulares, con las excepciones determinadas en aquel artículo.

La garantía de cumplimiento de contrato deberá presentarse sin límite temporal de validez.



## **ARTÍCULO 20. PREADJUDICACIÓN**

La preadjudicación se efectuará conforme al procedimiento establecido en el artículo 20 del Anexo I del Decreto N° 1.300/16.

## **ARTÍCULO 21. DEUDORES ALIMENTARIOS MOROSOS**

Los oferentes deberán cumplimentar las exigencias previstas por la Ley N° 13.074 y Decreto N° 340/04 en forma previa al dictado del acto administrativo de adjudicación por parte de la autoridad competente.

## **ARTÍCULO 22.- ADJUDICACIÓN**

La adjudicación debe realizarse a favor de la oferta más conveniente teniendo en cuenta para ello el precio, la calidad, la idoneidad del oferente, los costos asociados de uso y mantenimiento presentes y futuros y demás condiciones de la oferta.

Debe ser resuelta por acto administrativo dictado por la autoridad contratante, notificándose al adjudicatario y a quienes hayan efectuado impugnaciones o deducido pretensiones que se resuelvan en ese acto administrativo dentro de los siete (7) días hábiles de emitido el acto administrativo.

Obstará a la adjudicación toda distorsión significativa de la oferta en relación con precios de mercado del producto, bien o servicio ofrecido.

Se consideran incluidos en esta previsión todos los ocultamientos, incorrecciones y modificaciones injustificadas de los elementos y circunstancias que hacen a la aplicabilidad de las preferencias para contratación prioritaria, contempladas por el artículo 22 de la Ley que se reglamenta.



Podrán habilitarse, en particular para cada llamado o cuando la naturaleza del objeto de la prestación así lo justifique, métodos que posibiliten concluir la existencia de distorsiones significativas en las ofertas, que las hagan desestimables por evidenciar la imposibilidad de cumplimiento contractual

### **ARTÍCULO 23.- DECISIÓN DE DEJAR SIN EFECTO EL PROCEDIMIENTO**

Los organismos contratantes pueden dejar sin efecto el procedimiento de contratación en cualquier momento anterior al perfeccionamiento del contrato, sin que ello de lugar a indemnización alguna a favor de los interesados u oferentes.

### **ARTÍCULO 24.- PERFECCIONAMIENTO DEL CONTRATO**

El contrato se perfecciona con la notificación fehaciente de la orden de compra o venta al adjudicatario, o mediante la suscripción del instrumento respectivo, según corresponda. Formarán parte del mismo:

- 1) La Ley N° 13.981 y el Decreto Reglamentario N° 1.300/16
- 2) El Pliego de Bases y Condiciones Generales;
- 3) El Pliego de Bases y Condiciones Particulares, sus Especificaciones Técnicas y circulares dictadas de oficio o como respuesta a consultas;
- 4) La oferta y las muestras que se hubieren acompañado;
- 5) La adjudicación;
- 6) La orden de compra.

### **ARTÍCULO 25.-TRANSFERENCIA**



Se encuentra prohibida la cesión o subcontratación, salvo consentimiento expreso de la autoridad administrativa.

Toda tercerización, subcontratación, delegación o interposición en contravención a la prohibición precedente determinará la responsabilidad solidaria del contratante y del tercero por las obligaciones emergentes del contrato.

## **ARTÍCULO 26. MODIFICACIONES AL CONTRATO**

La autoridad administrativa contratante estará facultada para aumentar, disminuir y/o prorrogar el contrato.

El aumento o la disminución puede incidir sobre uno, varios o el total de los renglones, siempre y cuando el total resultante no exceda el porcentaje previsto.

La decisión de aumentar o disminuir en hasta un veinte por ciento (20%) la prestación objeto del contrato debe notificarse antes de la finalización del plazo de ejecución contractual.

El plazo para la nueva prestación será formalizado por acto administrativo suscripto por el funcionario con competencia y preverá la adecuación proporcional al período originalmente previsto.

El aumento o disminución superior al 20% deberá estar debidamente justificado por el organismo contratante y contar con la previa conformidad del cocontratante.

El cocontratante deberá manifestar su conformidad dentro de los cinco (5) días de notificada la solicitud, vencido dicho plazo sin que medie respuesta se entenderá que la misma no ha sido aceptada, no generando al proveedor ningún tipo de responsabilidad ni resultando pasible de ninguna penalidad.

En ningún caso podrá aumentarse el/los renglón/es por más de un 100% ni disminuirse por más de un 50%.



La decisión de prorrogar, tanto en contratos de suministros como en los de prestación de servicios y ya sea que incluya o no un aumento o disminución en la cantidad o nivel de prestaciones contratadas, deberá notificarse antes de la finalización del contrato.

La notificación de la orden de compra deberá producirse en un plazo no mayor a quince (15) días corridos computados desde el vencimiento del plazo de ejecución contractual y previa renovación de la garantía de cumplimiento del contrato, en su caso. Los efectos se retrotraerán a la fecha de efectiva vigencia de la modificación. Vencido el plazo indicado, el mantenimiento del contrato requiere nueva conformidad del contratante.

#### **ARTÍCULO 27.- ENTREGA**

Los adjudicatarios deben cumplir la obligación en la forma, fecha o plazos, lugar y demás condiciones establecidas en los Pliegos de Bases y Condiciones Particulares.

En caso de omisión del Pliego de Bases y Condiciones Particulares, se entenderá que:

- 1) El cumplimiento debe operar en un plazo de (10) días corridos, contados a partir del día siguiente al de recepción de la orden de compra o suscripción del instrumento respectivo, según corresponda;
- 2) El lugar de entrega es la sede de la autoridad administrativa de la jurisdicción;
- 3) Los elementos deben ser nuevos, sin uso y de primera calidad.

#### **ARTÍCULO 28. ENTREGAS PARCIALES**



Cuando el pliego de condiciones particulares prevea entregas parciales y provisión de bienes deberá estipular la modalidad del requerimiento, de la facturación y de cada plazo de cumplimiento.

#### **ARTÍCULO 29.- FLETE Y DESCARGA**

El flete y la descarga serán por cuenta del adjudicatario.

#### **ARTÍCULO 30.- CONFECCIÓN Y PRESENTACIÓN DE FACTURAS**

Las facturas deberán ser confeccionadas conforme los términos establecidos por la Administración Federal de Ingresos Públicos y presentadas en original en la repartición contratante, en la dependencia que al efecto se indique en las condiciones particulares. La presentación de la facturación deberá ser acompañada por:

- a) Original del parte de recepción definitiva.
- b) Fotocopia autenticada por escribano o certificada por el funcionario actuante del comprobante de pago del Impuesto sobre los Ingresos Brutos del último vencimiento operado al momento de presentar la factura;
- c) Fotocopia autenticada por escribano o certificada por el funcionario actuante de la última Declaración Jurada de Cargas Sociales (Formulario 931) vencida al momento de presentación de la factura y constancia de su pago;
- d) Constancia de su inscripción ante AFIP;
- e) Constancia de validez de la factura presentada;
- f) Otra documentación que exija el pliego particular o la normativa aplicable.

En cada factura debe constar:



- a) Número y fecha de la Orden de Compra, contrato o acto administrativo que corresponda;
- b) Número de Parte de Recepción Definitiva;
- c) Descripción de los conceptos facturados;
- d) Importe total de la factura;
- e) Todo otro requisito que establezca la Contaduría General de Contaduría, en su carácter de Órgano Rector del Subsistema de Contabilidad.

#### **ARTÍCULO 31.- PAGO**

El contratante cancelará sus obligaciones conforme las disposiciones establecidas en los apartados 2), 3) y 4) del punto III, del artículo 23 del Anexo I del Decreto N° 1.300/16.

#### **ARTÍCULO 32.- CLÁUSULA ANTICORRUPCIÓN**

Será causal determinante del rechazo de la oferta, en cualquier estado del procedimiento de contratación; así como causal de rescisión de pleno derecho del contrato, dar u ofrecer dinero o cualquier dádiva, a fin de que:

- a) Funcionarios o empleados públicos con competencia referida a una contratación, incurran en acciones u omisiones en el cumplimiento de sus funciones; o,
- b) Funcionarios o empleados públicos hagan valer la influencia de su cargo ante otro funcionario o empleado público con la competencia descrita, a fin de que éstos incurran en acciones u omisiones en el cumplimiento de sus funciones; o,
- c) Cualquier persona haga valer su relación o influencia sobre un funcionario o empleado público con la competencia descrita, a fin de que éstos incurran en acciones u omisiones en el cumplimiento de sus funciones.



Serán considerados sujetos activos de esta conducta quienes hayan cometido o intentaran cometer tales actos en interés del contratista, directa o indirectamente

### **ARTÍCULO 33.- RÉGIMEN DE RESPONSABILIDAD CON TERCEROS y PERSONAL**

Todo el personal afectado por el adjudicatario para el Cumplimiento de las obligaciones emergentes de la respectiva Contratación, y/o las relaciones jurídico contractuales generadas con terceros al efecto, carecerán de relación alguna con los sujetos contratantes.

Estarán a exclusivo cargo del adjudicatario los salarios, seguros, leyes y cargas sociales y previsionales así como cualquier otra erogación, sin excepción, vinculados con la ejecución contractual; quedando expresamente liberada la contratante por tales conceptos, y sin que se configure solidaridad alguna entre ambos.

La contratante quedará desligada respecto de todo litigio que eventualmente se genere por cuestiones de índole laboral entre el adjudicatario y su personal, como cualquiera otro conflicto que pudiera derivarse de la intervención de entidades sindicales y/o de aquellos organismos estatales de contralor de transgresiones a normas establecidas para el Orden laboral, previsional e impositivo que recaigan sobre el Adjudicatario.

### **ARTÍCULO 34. DAÑOS A TERCEROS**

El adjudicatario deberá adoptar todas las medidas de Seguridad que sean impuestas por la legislación vigente, para evitar daños a personas o cosas, y si ellos se produjeran, será responsable por el resarcimiento de los perjuicios que se generen.



### **ARTÍCULO 35. SEGUROS**

El Adjudicatario deberá contratar los seguros que se exijan para el desarrollo de su actividad y los que se requieran en el Pliego de Bases y Condiciones Particulares. El adjudicatario será el único responsable de los perjuicios que ocasionare la inobservancia de la contratación de los Seguros exigidos, quedando la contratante exenta de toda responsabilidad respecto de cualquier siniestro que se produjera.

### **ARTÍCULO 36. INCUMPLIMIENTOS**

El incumplimiento de las obligaciones contraídas por los oferentes, preadjudicatarios o adjudicatarios dará lugar a la aplicación de las penalidades y sanciones previstas por los artículos 24 y 25 del Anexo I del Decreto N° 1.300/16.



## CAPITULO II

### PLIEGO DE BASES Y CONDICIONES PARTICULARES PARA LA CONTRATACION

#### DE BIENES Y SERVICIOS

#### **ARTÍCULO 1º. OBJETO DE LA CONVOCATORIA.**

El presente llamado a Licitación Pública tiene por objeto la contratación de un servicio integral, para los Casinos Oficiales de la Provincia de Buenos Aires, a saber: Casino Central de Mar del Plata, Casino Anexo III de Mar del Plata (Hotel Hermitage), Casino de Miramar, Casino de Monte Hermoso, Casino de Pinamar, Casino de Tigre, Casino de Tandil; excluyéndose de la misma al Casino de Necochea, Casino de Valeria del Mar, Casino de Mar de Ajó, Casino Anexo I de Mar del Plata (Hotel Sasso) y al Casino de Sierra de la Ventana. La contratación incluirá los siguientes servicios, los que serán desarrollados en el Capítulo III, del Pliego de Bases y Condiciones Técnicas:

- Instalación, renovación, funcionamiento, mantenimiento y reparación del parque de máquinas electrónicas de juego de azar automatizadas, existente en los Casinos de la Provincia.
- Implementación, funcionamiento y mantenimiento de un Sistema de Control On line para las Máquinas Electrónicas de Juego de Azar Automatizadas existentes en los Casinos de la Provincia.
- Implementación, funcionamiento y mantenimiento de un Sistema de monitoreo ambiental.
- Implementación, funcionamiento y mantenimiento de un Sistema de control de movimiento físico de valores.
- Implementación, funcionamiento y mantenimiento de un Sistema de comunicación e infraestructura tecnológica.



- Provisión, instalación, configuración, funcionamiento, capacitación, mantenimiento y renovación de las redes Hardware, Software, infraestructura tecnológica necesaria para el funcionamiento de los Casinos y su interoperación con el INSTITUTO.
- Provisión, mantenimiento y renovación de Mesas de Juego de Paño, insumos y accesorios.
- Provisión, mantenimiento y renovación de contadoras, clasificadoras de billetes y tickets y detectoras de billetes falsos.
- Provisión, funcionamiento, capacitación y renovación de un Sistema de Control por Video.
- Instalación, funcionamiento y mantenimiento de sistemas de control de acceso.
- Implementación Sistema de cobro de entradas de ingresos a los Casinos a licitarse.
- Provisión y mantenimiento de Servicios de Limpieza, Emergencias y Seguridad.
- Provisión de Servicios Complementarios.
- Provisión de Servicios de Restaurantes, Bares y Confiterías.
- Provisión y renovación del mobiliario de las dependencias internas y cofres para los vestuarios del personal.
- Mantenimiento integral de la totalidad de los inmuebles objeto de la presente licitación.
- En materia de Infraestructura: Se prevé la refacción, construcción y/o cesión de espacios destinados al funcionamiento de los Casinos objeto de la presente licitación.

En el Casino Anexo III de Mar del Plata (Hotel Hermitage) y en el Casino Central de Mar del Plata, se deberá realizar una obra de remodelación de sus estructuras edilicias, en tanto, para los Casinos de Tigre, Pinamar, Tandil, Miramar y Monte Hermoso, se requerirá al adjudicatario, la provisión de espacios aptos para el funcionamiento de cada Casino, mediante la construcción y/o cesión de los mismos.

Tanto los casos de construcción como los de remodelación deberán contemplar salas de juego, dependencias internas y fachadas externas.



El presente llamado a licitación, estará integrado por tres renglones, pudiendo los oferentes efectuar ofertas por uno, varios o todos, ello conforme surge del Art. 17 ap. 4 del Anexo I del Decreto N° 1300/16.

Dichos renglones, se conforman de la siguiente manera:

RENGLON N°1: Casino de Tigre y Casino de Pinamar

RENGLON N°2: Casino de Tandil, Casino de Miramar y Casino Anexo III de Mar del Plata (Hotel Hermitage)

RENGLON N°3: Casino Central de Mar del Plata y Casino de Monte Hermoso.

Los casinos mencionados precedentemente, continuarán su normal funcionamiento, independientemente de las obras de construcción y de remodelación a realizarse.

Para los casos de aquellas salas en las cuales el adjudicatario deba realizar obras de Remodelación/Refacción, se acordará un plan de acción con el INSTITUTO; en el cual se establezca el cronograma a ejecutar. Se fijará como objetivo primordial el cumplimiento de los plazos de finalización de obras definidos en la presente Licitación, y evitar entorpecer el correcto funcionamiento de las Salas.

Dado que el INSTITUTO explota, administra y controla las actividades referentes a todos los Casinos Oficiales de la Provincia (conforme Decreto N° 1170/92), le requerirá al adjudicatario un plan de explotación de todos los servicios objeto de la presente licitación, interviniendo y autorizando las políticas de comercialización de los mismos.

Será obligación del adjudicatario, el pago de los consumos de los servicios públicos en cada una de las Salas de juego, a saber: Energía eléctrica, gas natural, agua corriente, servicios sanitarios, servicio de internet, y tasas municipales existentes o



que en un futuro los municipios impongan sobre los inmuebles asiento de las salas de juego.

El INSTITUTO, como Autoridad de Aplicación, será el responsable de establecer y homologar, a través de su personal técnico, las especificaciones técnicas y profesionales de cada ítem y de dirimir toda circunstancia que no se encuentre determinada en el presente pliego de condiciones.

## **ARTÍCULO 2º. PLAZO DE VIGENCIA.**

El plazo de vigencia de la presente licitación, será de veinte (20) años, contados a partir de la fecha de suscripción del contrato, con posibilidad de prorrogarlo por un (1) año adicional, a opción del INSTITUTO, ello en concordancia con lo estipulado en el Artículo 7 inciso f) de la Ley 13.981. En caso de ejercer dicha opción, el INSTITUTO deberá notificar al adjudicatario con una antelación no menor a los ciento ochenta (180) días previos a la finalización del plazo de duración del servicio, conforme lo establecido en el Artículo 25 del Pliego de Bases y Condiciones Generales.

Al finalizar el plazo de vigencia de la presente licitación, los espacios provistos por el adjudicatario, y todo aquello que se encontrare construido en los mismos, quedará en propiedad del Adjudicatario.

En tanto, pasará a formar parte del patrimonio del INSTITUTO la totalidad del equipamiento mobiliario existente; la totalidad del parque de Máquinas Electrónicas de Juegos de Azar Automatizadas (estableciéndose que el promedio de la antigüedad del parque de máquinas de cada Sala tomada individualmente, no podrá superar los cinco (5) años al momento de transferir las mismas), y todo el equipamiento tecnológico (hardware y software) que hubiere incorporado el adjudicatario a los efectos de la realización del objeto de la licitación, incluidos los



sistemas y las licencias necesarias para su operación, servidores y demás dispositivos de infraestructura y redes, así como también los firewall.

De la misma manera, será propiedad del INSTITUTO, durante la vigencia y una vez finalizada la presente licitación, la totalidad de la información resultante de la operación de las Salas de Casino, contenida en la infraestructura tecnológica y en los sistemas instalados en las Salas de Casino y/o en el INSTITUTO. Debiendo garantizar el Adjudicatario en todo momento la integridad, confidencialidad y disponibilidad de esta información.

### **ARTÍCULO 3º. EXCLUSIVIDAD.**

Durante el plazo de vigencia del contrato y su eventual prórroga, el INSTITUTO no autorizará el funcionamiento de Salas de Bingo adicionales, ni el funcionamiento de Máquinas Electrónicas de Juegos de Azar y/ o Mesas de Paño que no fueren para Salas de Casinos Oficiales, en los Partidos donde se encuentran las Salas de Juegos comprendidas en el presente.

### **ARTÍCULO 4º. ADQUISICIÓN DEL PLIEGO.**

Los Interesados podrán consultar el Pliego de Bases y Condiciones en el sitio Web de la Provincia de Buenos Aires [www.gba.gob.ar](http://www.gba.gob.ar).

A los efectos de poder realizar una oferta, se deberá adquirir un ejemplar del mismo, en el Área Contrataciones del INSTITUTO Provincial de Lotería y Casinos, sito en la calle 46 n° 581 Primer Piso de La Plata, Provincia de Buenos Aires, en el horario de 09:00 a 13:00 horas.

Cuando el Oferente esté integrado por dos o más personas jurídicas, es suficiente que una de ellas hubiera adquirido el Pliego. En tal caso, quien lo haya adquirido deberá solicitar que el correspondiente recibo se extienda a su nombre y que se agregue el aditamento “y otros”.



Las comunicaciones que se realicen entre el contratante y los interesados, oferentes, preadjudicatarios y adjudicatarios, serán efectuadas al domicilio electrónico dispuesto por el artículo 12 del Decreto Reglamentario N° 1300/16, que a tal fin deberán constituir.

#### **ARTÍCULO 5º. CONSULTAS Y ACLARACIONES.**

Los interesados que hayan adquirido el Pliego podrán formular consultas aclaratorias por escrito, hasta diez (10) días antes de la fecha de apertura del primer sobre. A los efectos del cómputo del plazo, no se tendrá en cuenta el día de la apertura de ofertas. Las consultas se realizarán por escrito y deberán ser presentadas en el Área Contrataciones de la Dirección Provincial de Administración y Finanzas del Instituto Provincial de Lotería y Casinos, sito en calle 46 N° 581 de la Ciudad de La Plata, Provincia de Buenos Aires.

Todas las consultas y sus respuestas, serán incluidas en la documentación licitatoria como integrante de la misma y se notificará a todos los interesados que hubieren adquirido el Pliego de Bases y Condiciones, en la forma establecida en el artículo anterior.

Sin perjuicio de ello, el INSTITUTO podrá aclarar de oficio conceptos particulares o generales del pliego, emitiendo las circulares aclaratorias pertinentes, que serán publicadas en el sitio Web de la Provincia de Buenos Aires y deberán ser notificadas a todos los adquirentes del pliego en la forma establecida en el artículo anterior.

#### **ARTICULO 6º. CONTRAPRESTACIÓN.**

En contraprestación por la provisión de bienes, servicios y cesión de uso objeto de la presente Licitación; el INSTITUTO abonará al adjudicatario como única retribución, un porcentaje de la rentabilidad mensual producida por la explotación



de las Máquinas Electrónicas de Juegos de Azar que se instalen en los casinos referidos en el artículo 1° y que el oferente deberá cotizar. Dicha cotización deberá expresarse en porcentaje.

A tales efectos, se acompaña como Anexo IV del presente pliego la rentabilidad correspondiente al año 2017 de las Máquinas Electrónicas de Juegos de Azar Automatizadas en los Casinos Oficiales, proyectada por este INSTITUTO. Se entiende por rentabilidad a la diferencia existente entre el total apostado y el total pagado en concepto de premios.

Quedará a cargo del adjudicatario el pago del Impuesto al Valor Agregado (IVA), como así también cualquier otro impuesto, tasa o gravamen existente o que se cree en un futuro.

#### **ARTÍCULO 7º. OFERENTES.**

Sin perjuicio del cumplimiento de los recaudos requeridos por las Condiciones Generales, sólo podrán participar los Oferentes que se indican en el presente artículo, quienes acreditarán las condiciones de capacidad técnica y financiera que se establecen en estas Condiciones Particulares (requisitos de admisibilidad).

7.1. Podrán participar en calidad de Oferente las sociedades comerciales regularmente constituidas en el país de acuerdo a las prescripciones de la Ley Nro. 19.550, que habiendo adquirido el Pliego reúnan las condiciones de admisibilidad exigidas.

7.2. También podrán participar las sociedades que se encuentren vinculadas por un Contrato de Unión Transitoria (U.T.), las que se encuentren en la etapa de formación del mismo, o aquellas que hayan asumido el compromiso de constituir la en caso de resultar adjudicatarias.

En los supuestos de presentaciones de U.T., las sociedades integrantes, serán solidaria e ilimitadamente obligadas y responsables por el cumplimiento del contrato



y por todos los actos y hechos que pudieran producir perjuicio al INSTITUTO y/o a cualquier otra persona con motivo u ocasión de ello, sin beneficio de división y excusión. Este extremo deberá ser instrumentado mediante la forma de Declaración Jurada firmada por cada sociedad integrante de la U.T., en la que conste que asume solidaria e ilimitadamente, sin beneficio de división y excusión de la responsabilidad por el cumplimiento del contrato y por todos los actos y hechos que pudieran producir perjuicio al INSTITUTO y/o a cualquiera otra persona con motivo u ocasión de ello. Este instrumento deberá contener todos los extremos que acrediten la personería y facultades del firmante para obligar a su representada. Las sociedades constituidas en el extranjero podrán participar exclusivamente como integrantes de una U.T., y en la medida que la/s restante/s sociedad/es participantes de una U.T. se encuentre/n regularmente constituida/s en el país.

7.3. El objeto social de las sociedades postulantes, así como el establecido en el contrato de U.T., deberá ser adecuado a los fines de la presente selección. Los integrantes de la U.T. deberán ser únicamente quienes presenten la oferta.

7.4. Los oferentes asumen la obligación que durante el plazo de vigencia establecido en el artículo 2° del presente, no introducirán modificaciones estatutarias que importen alteraciones en las responsabilidades comprometidas en el presente Pliego y en el contrato a suscribir.

#### **ARTÍCULO 8°. IMPEDIMENTOS PARA PRESENTARSE EN LA LICITACIÓN.**

Sin perjuicio de lo establecido en el art. 16, apartado III del Decreto N° 1.300/16, están excluidos para participar de la licitación quienes se encuentren comprendidos en los siguientes supuestos:

a) Se hallaren actualmente en estado de inhibición, concurso preventivo o acuerdo preventivo extrajudicial, quiebra, con o sin continuidad de la explotación, o liquidación sin quiebra. Este impedimento también comprende a aquellas sociedades cuyos directores, accionistas mayoritarios, o empresas controlantes o



controlada se encontraren en la actualidad en algunas de las situaciones descriptas precedentemente.

b) Los ex permisionarios, ex contratistas o ex agentes oficiales del INSTITUTO que en los últimos diez (10) años hubieren sido pasibles de la sanción de revocación por causas imputables a ellos.

c) Quienes a la fecha de la apertura del sobre N° 1 se encontraren excluidos o suspendidos del Registro de Proveedores y Licitadores del Estado.

d) Los oferentes que a la fecha de efectuar la oferta, exploten en el mismo Municipio en que se hallare la Sala de Casino a ofertar, el juego de azar denominado “Lotería Familiar”, “Lotería Familiar Gigante”, o “Bingo”, conforme Artículos 1 y 4 de la Ley N° 11.018.

#### **ARTICULO 9º. PRESENTACION DE LAS PROPUESTAS.**

La oferta deberá presentarse hasta el día y hora señalado por el INSTITUTO.

La presente Licitación se realizará de acuerdo con el mecanismo de etapa múltiple. Ambos sobres deberán estar cerrados, debidamente firmados por el proponente o apoderado y lacrados con indicación en su exterior del número de la Licitación Pública para la cual se presenta y el nombre del oferente, debiéndose consignar en el exterior del SOBRE N° 1: “SOBRE N° 1: ANTECEDENTES Y PROPUESTA TECNICA” y en el exterior del SOBRE N° 2: “SOBRE N° 2: OFERTA ECONOMICA”.

Ambos sobres deberán estar contenidos en un único paquete o sobre rotulado en la forma que se indica seguidamente:

- Área Contrataciones de la Dirección Provincial de Administración y Finanzas del INSTITUTO, sito en la calle 46 N° 581 entre las calles 6 y 7 de la Ciudad de La Plata – Provincia de Buenos Aires.



- Expediente Nro.:
- Licitación Pública Nro.:

La propuesta deberá confeccionarse y presentarse conforme los términos establecidos por el Artículo 17, Apart. 4 "Ofertas: "Presentación", "Contenido" y "Documentos a acompañar" (Decreto Reglamentario 1.300/16).

En caso de duda o discrepancia, el texto del original prevalecerá sobre el de las copias.

La documentación exigida en el Pliego de Bases y Condiciones deberá ser presentada en original o en copia certificada por escribano público. Si el escribano fuere de extraña jurisdicción, deberá ser legalizada por el Colegio de Escribanos correspondiente. La documentación proveniente del extranjero deberá ser autenticada en legal forma en el país de origen, con la apostilla correspondiente – en el caso de países firmantes de la Convención Suprimiendo la exigencia de Legalización de los Documentos Públicos Extranjeros adoptada por la Conferencia de La Haya de Derecho Internacional Privado – o mediante legalización del Ministerio de Relaciones Exteriores y Culto.

La documentación extranjera podrá ser presentada en su idioma de origen, siempre que se adjunte la correspondiente traducción al castellano, efectuada por traductor público matriculado, debidamente legalizada.

En caso de adjuntarse folletos, catálogos o medios audiovisuales, para una mejor comprensión de la presentación los mismos deberán ser firmados y foliados correlativamente, conforme lo previsto en el el pliego.

#### **ARTÍCULO 10°. DOCUMENTACIÓN A ACOMPAÑAR.**

Los postulantes deberán presentar en el contenido del Sobre N° 1:



- Índice con la identificación y ubicación de la totalidad de los documentos acompañados en la Oferta.
- Carta de presentación de la oferente, detallando la razón social, domicilio social y constituido, CUIT, breve referencia de antecedentes comerciales y la decisión de participar de la Licitación aceptando los términos del Pliego de Bases y Condiciones. En caso de tratarse de una U.T., la carta de presentación deberá encontrarse suscrita por parte de cada uno de los integrantes de la misma y por el representante de la U.T..
- El Pliego de Bases y Condiciones Generales, Particulares y todos los anexos que forman parte de la presente licitación, conjuntamente con las circulares y/o aclaraciones que pudiesen ser emitidas por el INSTITUTO, debidamente firmadas en todas sus fojas, en anverso y reverso, por el proponente o apoderado, como forma de exteriorizar su voluntad de someterse explícitamente a las condiciones establecidas en los documentos que componen la compulsa.
- El recibo original de adquisición del Pliego a nombre del Oferente.
- Constancia de inscripción ante el Registro de Proveedores y Licitadores del Estado de la Provincia de Buenos Aires, o constancia de inicio del trámite, mediante la presentación del formulario de inscripción. En tal caso, es condición para la preselección que el proveedor se encuentre inscripto en el Registro de Proveedores y Licitadores.
- Denunciar domicilio real o social, fijar domicilio legal en el ámbito de la Provincia de Buenos Aires y constituir domicilio electrónico, donde serán válidas todas las notificaciones a realizar en el marco de la presente licitación pública.
- Copia certificada del Contrato o Estatuto Societario debidamente inscripto del oferente, como así también del acta de formación de la Unión Transitoria y de los poderes que se presentasen, según el caso.



- Documentación que acredite la titularidad del capital social o tenencia accionaria del Oferente. Asimismo, deberá presentar un diagrama documentado detallando la estructura legal del mismo, partiendo de la persona jurídica que presenta la oferta y sus integrantes hasta la(s) persona(s) física(s) que finalmente la controlen. De tratarse en este último caso de un fondo de inversión, deberá detallarse el país donde está registrado, sus beneficiarios y la(s) persona(s) físicas que tienen poder de decisión sobre el mismo. En caso de las sociedades cuyas acciones se comercialicen en el mercado de valores, deberá presentar certificación que acredite dicha situación.
- Documentación social que acredite la actual composición del órgano de administración y fiscalización. Nómina de los actuales integrantes de sus órganos de administración y fiscalización, con el respectivo detalle de los datos de identificación (fotocopia del documento de identidad, fecha de nacimiento, filiación, estado civil y nombre del cónyuge, ocupación principal y domicilio real) y documentación que acredite el período de vigencia de su mandato. Cuando la formulación y presentación de la Oferta se efectuara por medio de apoderado se deberá acreditar mediante poder que confiera la representación, en forma expresa, a la persona que designe el oferente para ello, con facultades explícitas para asumir las obligaciones emergentes de la Licitación. Las personas nominadas serán consideradas Representantes Legales o Apoderados del oferente.
- Copia de las actas de Asambleas Ordinarias y Extraordinarias celebradas en los tres (3) últimos ejercicios, de así corresponder según su antigüedad, y del Registro de Accionistas.
- Copia del acta del órgano de administración con la decisión de participar de la Licitación como oferente y asumir todas las obligaciones requeridas por el Pliego. En caso de una U.T., el acta de los integrantes de la misma deberá, a su vez, contener la decisión expresa de concurrir en forma conjunta en la



Licitación, y asumir todas las obligaciones requeridas por el Pliego en forma solidaria con los restantes integrantes de la U.T.

- Declaración Jurada, por parte de los oferentes, integrantes de los miembros del directorio y accionistas controlantes de no hallarse incurso en ninguna de las prohibiciones e incompatibilidades para ser oferente, de conformidad a lo establecido en el artículo 16 inciso III del decreto 1300/16.
- Constancia de inscripción en Administración Federal de Ingresos Públicos. CUIT.
- Certificado fiscal para contratar expedido por la Administración Federal de Ingresos Públicos.
- Formulario A-404 aprobado por la Resolución Normativa N° 50/2011 de la Agencia de Recaudación de la Provincia de Buenos Aires.
- Constancia debidamente certificada por la entidad, que acredite titularidad de cuenta bancaria en el Banco de la Provincia de Buenos Aires o Bancos especialmente habilitados por el Ministro de Economía, con indicación de su CBU.
- Las personas físicas integrantes del órgano de administración y de fiscalización, y las personas físicas controlantes del oferente, deberán presentar:
- Certificado de libre deuda expedido por el Registro de Deudores Alimentarios Moroso, Ministerio de Justicia, Ley Nro. 13.074 y decreto 340/04.
- Certificado de antecedentes penales expedido por la Dirección Nacional del Registro Nacional de Reincidencias y Estadística Criminal.
- Declaración Jurada de no integrar los órganos de administración y de fiscalización de Oferentes que integren otra oferta.



- Descripción de antecedentes generales sobre la capacidad empresarial, económica y financiera del postulante.
- Estados Contables (Estado de situación Patrimonial, Estado de Resultados, Estado de Evolución del Patrimonio Neto, Estado de Flujo de Efectivo, Anexos, Notas y Memoria) de los últimos tres (3) ejercicios económicos de la empresa, si correspondiere. Los estados contables y declaraciones patrimoniales deberán estar aprobados por la asamblea de accionistas, auditados por contador público independiente y legalizado por el Consejo Profesional competente. En caso de tratarse de una U.T., deberán acompañar los Estados Contables correspondientes a cada uno de sus miembros.
- Estado de situación patrimonial y financiero actualizado al anteúltimo mes vencido anterior a la fecha de presentación de la propuesta, indicándose el criterio de valuación utilizado. El mismo deberá reflejar las deudas devengadas a favor del Fisco Nacional, Provincial y Municipal. También deberá detallar las mantenidas con entidades financieras con especificación de plazos y garantías constituidas. En caso de tratarse de una U.T., deberán acompañar el Estado de situación patrimonial y financiero actualizado mes vencido anterior a la fecha de presentación de la propuesta, indicándose el criterio de valuación utilizado, correspondiente a cada uno de sus miembros. Aquellas empresas que realicen oferta pública de acciones, podrán, en su defecto, acompañar el último balance trimestral presentado ante la autoridad de aplicación.
- Las empresas que hayan suscripto un compromiso o contrato de Unión Transitoria, acompañarán copia de los mismos y agregarán toda la documentación relativa a sus integrantes como concurrentes individuales, según lo previsto en los incisos precedentes. Dicho contrato o compromiso de constitución deberá contener, además de las previsiones dispuestas en el art. 1.464 del Código Civil y Comercial de la Nación, las siguientes cláusulas:



1.- El compromiso expreso de responsabilidad solidaria e ilimitada de todas y cada una de las sociedades que la conforman, para el cumplimiento de todas las obligaciones legales y contractuales conforme a lo establecido en el Presente Pliego de Bases y Condiciones.

2.- El compromiso de mantener la vigencia de la asociación hasta que se hayan cumplido todas las obligaciones contractuales.

3.- Designación de uno o más representantes legales que acrediten facultades suficientes para obligar a su mandante.

- Notas con referencias bancarias, financieras y comerciales, demostrativas de la capacidad económica y financiera del oferente. El INSTITUTO se reserva el derecho de solicitar la información y/o documentación complementaria que considere necesaria, destinada a la determinación de la capacidad económica, técnica y legal del postulante, sus accionistas, empresas, personas o fondos de inversión controlantes y casas matrices y cualquier otro dato que estime necesario.
- Los oferentes deberán presentar un detalle documentado sobre el financiamiento de la inversión propuesta. Si se trata de fondos propios líquidos, los mismos deberán surgir de los estados contables presentados. Si se trata de créditos a obtener de terceros, deberán acompañar una manifestación escrita de los mismos donde se detalle el monto de financiar, los plazos, tasas de interés y garantías exigidas; si se trata de fondos a generarse en las operaciones de sus Integrantes, los mismos deberán ser los correspondientes al período de 12 meses terminado a la fecha de los estados contables presentados. Si se trata de aumentos de capital, la(s) persona(s) física(s) o fondo(s) de inversión controlantes deberán acreditar la tenencia de fondos líquidos disponibles, los cuales deben estar incluidos en las correspondientes declaraciones juradas presentadas ante los organismos encargados de la administración tributaria.



- Acreditación de constitución de la garantía a que se refiere el artículo 19 apartado 1 inciso a) del Anexo I del Decreto N° 1300/16.
- Maestro de máquinas que pondrán en explotación con detalles que incluyan marca, modelo, año de fabricación, función AFT, protocolo SAS 5.0 o superior, certificado de GLI, precio de lista del distribuidor oficial en Argentina.
- Certificado de homologación del Sistema On-line conforme los requerimientos del presente pliego y cualquier otra certificación adicional con la que el sistema cuenta.
- Documento funcional del Sistema On-line para la evaluación de prestaciones y evaluación del cumplimiento del Reglamento de MEJAAs en los Casinos de la Provincia de Buenos Aires según resolución vigente.
- Esquema completo de conectividad entre la sala de juego y el Instituto.
- Propuesta técnica conforme al siguiente detalle y lo previsto en las especificaciones técnicas en su capítulo correspondiente:

Según corresponda:

1.1 Supuesto de cesión: La documentación que acredite la disponibilidad de los espacios que ofrece para ceder su uso para la instalación de las Salas que se obliga a proveer, mediante título de escritura a su nombre, boleto de compraventa, contrato de locación o compromiso irrevocable de venta, locación, comodato o cesión, a favor del Oferente para el caso de resultar adjudicatario de la licitación. Características, calidad, funcionalidad y dimensiones de los espacios a ceder para el funcionamiento de las salas de juegos.

1.2 Supuesto de construcción y/o cesión: La documentación que acredite la disponibilidad de los espacios que ofrece para la construcción y/o cesión de las Salas que se obliga a proveer, mediante título de escritura a su nombre, boleto de compraventa o compromiso irrevocable de venta, a favor del Oferente para el caso



de resultar adjudicatario de la licitación. El proyecto de construcción indicando características, calidad, funcionalidad y dimensiones de los espacios a construir para el funcionamiento de las salas de juegos.

- Propuesta con detalle de inversión a realizar, por ítem, por sala y plazos para la realización de la misma.
- Cronograma de realización de las tareas comprometidas.
- Planos de arquitectura y de Ingeniería.
- Maqueta digital del establecimiento en el que funcionará el casino
- Programas de inversiones del proyecto.
- Informe económico-financiero del proyecto
- Plan de seguridad para el funcionamiento del casino.

#### **ARTÍCULO 11º: OFERTA ECONOMICA. COTIZACION.**

Los postulantes deberán presentar en el contenido del SOBRE N° 2, la planilla de cotización del precio ofrecido – conforme Anexo II del presente pliego-, las cuales serán evaluadas una vez finalizado el procedimiento de evaluación del sobre N° 1.

#### **ARTICULO 12º: MANTENIMIENTO DE OFERTA**

La presentación de la propuesta conlleva la obligación de mantener la misma por el término de ciento ochenta (180) días corridos contados a partir del acto de apertura. A tal efecto el oferente deberá constituir la garantía de mantenimiento de oferta indicada en el Artículo N° 18 del presente pliego.



Producido el vencimiento del plazo del mantenimiento de oferta, el mismo quedará automáticamente prorrogado por el término de 30 (treinta) días corridos. Las siguientes prórrogas deberán contar con la manifestación expresa del oferente.

### **ARTÍCULO 13º: APERTURA DE SOBRE N° 1. ACTA. MANIFESTACIONES.**

La presentación de las propuestas deberá efectuarse en el Área Contrataciones de la Dirección Provincial de Administración y Finanzas, en la sede del INSTITUTO, sita en calle 46 N° 581, Primer Piso, de la ciudad de La Plata, Provincia de Buenos Aires, hasta una hora antes del día y la hora fijada para la apertura. Vencido este plazo no se admitirán más propuestas.

El día, hora y en el lugar indicado en el aviso de llamado a Licitación Pública o el que fije y notifique a los interesados el INSTITUTO en caso de prórroga de plazo o cambio de lugar, y con la presencia de autoridades del INSTITUTO, de la Escribanía General de Gobierno y de los Oferentes que concurran, se procederá a la apertura de las ofertas recibidas.

Las ofertas se deberán presentar en sobre con o sin membrete del oferente, o en cajas o paquetes si son voluminosas, perfectamente cerrados y por duplicado, debiendo contener en su frente o cubierta la indicación de:

Organismo contratante y domicilio;

Número de expediente;

Tipo y número que identifica la contratación.

Las ofertas serán admitidas hasta el día y hora fijados para la apertura del acto.

La presentación de ofertas implica el conocimiento y aceptación del Pliego de Bases y Condiciones, el sometimiento a todas sus disposiciones, a las de la Ley 13981 y del Decreto 1300/16.



Las propuestas se presentarán preferentemente en cualquiera forma impresa y cada hoja será firmada por el proponente o su representante legal.

Las enmiendas y raspaduras en partes esenciales de la oferta, deben ser debidamente salvadas.

El error evidente podrá ser corregido de oficio por la Comisión de Preadjudicación antes de notificar su dictamen y por el oferente hasta el mismo momento. Todo otro tipo de error en la cotización importa la desestimación de la oferta o la aplicación de las penalidades previstas para la deserción, en su caso.

Se comenzará con la apertura del SOBRE N° 1 de las Ofertas, siguiendo el orden en que hayan sido presentadas en el INSTITUTO.

Previo a la finalización del acto, se procederá a la reserva del SOBRE N° 2 de cada Oferente, para la apertura que se celebrará de conformidad a lo establecido en el artículo 15 de este Pliego de Condiciones Particulares. Se labrará acta donde se dejará constancia de lo actuado, que deberán suscribir los presentes.

#### **ARTÍCULO 14°. PROCEDIMIENTO DE EVALUACIÓN DEL SOBRE N° 1.**

La Comisión de Preadjudicación podrá requerir a los oferentes información complementaria sobre las propuestas, información que deberá ser brindada por escrito dentro de los cinco (5) días de requerida, lo cual no implicará de ninguna forma modificación de la propuesta original o las bases de la contratación. Se agregará al expediente copia de la nota de requerimiento, y el informe recibido, que quedará a la vista de los demás oferentes. El incumplimiento de la obligación de brindar información complementaria, facultará a desestimar la oferta, salvo que se justifique el atraso o la imposibilidad de cumplimentarla a juicio de la Comisión de Preadjudicación.



La Comisión de Preadjudicación, podrá requerir informes a terceros y la exhibición de libros y comprobantes para verificar todos los requisitos de las ofertas, en cualquier momento del proceso licitatorio.

Reunida la documentación necesaria, la Comisión de Preadjudicación procederá al análisis y evaluación del SOBRE N° 1, debiendo emitir dictamen fundado dentro de un plazo de treinta (30) días. En el dictamen de evaluación se deberá considerar:

- Existencia de causales de rechazo de las Ofertas.
- La desestimación de Ofertas que no cumplieren con el Pliego de Bases y Condiciones.
- Puntaje de evaluación correspondiente al SOBRE N° 1, calificando para la apertura y análisis del SOBRE N° 2, aquellas ofertas que alcancen, el puntaje mínimo establecido, de acuerdo a los criterios de evaluación previstos en el artículo 17° y los requisitos exigidos.

El dictamen de la Comisión de Preadjudicación será notificado a los oferentes al domicilio electrónico. Estos tendrán tres (3) días hábiles para formular observaciones e impugnar al dictamen.

De las impugnaciones presentadas, tomará nueva intervención la Comisión de Preadjudicación, y se dará intervención de manera simultánea a los organismos de asesoramiento y control de la provincia, quienes deberán expedirse sobre el particular.

Dentro de los diez (10) días de recibidas las actuaciones, se dictará un acto administrativo donde resolverá acerca de:

- El acogimiento o rechazo de las impugnaciones que se hubieren deducido, disponiendo la devolución de la garantía en el único caso de que la impugnación haya ocasionado el rechazo de la Oferta impugnada o si ésta hubiere sido declarada inadmisibile.
- La admisibilidad de las Ofertas presentadas y su puntuación.



Posteriormente se fijará la fecha, hora y lugar para la apertura del SOBRE N° 2.

Las Ofertas rechazadas o desestimadas, con la garantía de mantenimiento de oferta, sin que se proceda a la apertura del SOBRE N° 2 de las mismas, quedarán a disposición del interesado para su retiro por el plazo de quince (15) días, vencido el cual se procederá a su destrucción.

#### **ARTÍCULO 15°: APERTURA DEL SOBRE N°2.**

15.1. El día, hora y lugar fijado en el acto administrativo correspondiente, se procederá a la apertura del SOBRE N° 2, que contiene la Oferta Económica, de aquellas ofertas que hubieren sido calificadas como admisibles, en presencia de las autoridades del INSTITUTO, de la Escribanía General de Gobierno y de los Oferentes que concurran.

15.2. Se comenzará con la apertura del SOBRE N° 2, siguiendo el orden de numeración de las Ofertas y se labrará acta a tal efecto, que deberán suscribir los presentes.

#### **ARTÍCULO 16°: PROCEDIMIENTO DE EVALUACIÓN DEL SOBRE N° 2.**

Determinada la fecha de la apertura del SOBRE N° 2, la Comisión de Preadjudicación procederá a evaluar la propuesta económica, conforme a los criterios descriptos en el artículo 17°, estableciéndose un orden de prelación de acuerdo al puntaje obtenido, para lo cual tendrá un plazo de quince (15) días.

El dictamen de la Comisión de Preadjudicación será notificado a los oferentes al domicilio electrónico. Estos tendrán tres (3) días hábiles para formular observaciones e impugnaciones al dictamen.

De las impugnaciones presentadas, tomará nueva intervención la Comisión de Preadjudicación, y se dará intervención de manera simultánea a los organismos de



asesoramiento y control de la provincia, quienes deberán expedirse sobre el particular.

En caso de paridad de ofertas, la preadjudicación corresponde a la propuesta que ofrezca mayor cantidad de elementos de origen nacional. De subsistir el empate se solicitará a los proponentes que, por escrito y dentro de los tres (3) días, formule una mejora de precios. Las nuevas propuestas que se presenten, serán abiertas en el lugar, día y hora establecidos en el requerimiento, labrándose el Acta pertinente.

El silencio del oferente invitado a desempatar, se entiende como mantenimiento de la propuesta sin modificación.

De mantenerse el empate, se preadjudicará en base a otras ventajas como: mayor de criterios sustentables incorporados a la oferta, mayor cantidad de elementos de mejor calidad o características diferenciales similares.

Si ninguno de estos criterios resultare de aplicación, la Comisión de preadjudicación procederá a realizar un sorteo público de las ofertas empatadas. Para ello deberá fijarse día, hora y lugar del sorteo público y notificar a los oferentes llamados a desempatar.

## **ARTICULO 17°. EVALUACION DE LAS PROPUESTAS**

### **17.1. Evaluación de las Ofertas:**

Sólo serán admitidas aquellas Ofertas que cumplan con todos los requisitos exigidos y estén en un todo de acuerdo a las Condiciones del Pliego.

Se considerarán calificados por el sobre N°1, y en condiciones de pasar a la apertura del sobre N°2, aquellos Oferentes que obtengan un puntaje final en el Sobre N°1 igual o superior a treinta (30) puntos.

La evaluación de los sobres 1 y 2 se efectuará conforme a los siguientes criterios:

### **Grilla de evaluación de experiencia y capacidad técnica**

38



Puntaje 100

a) Experiencia demostrable en la explotación y administración de Casinos:

Máximo ocho (8) puntos.

Los ocho (8) puntos de este ítem, se dividen en dos sub- ítems:

a.1- Antigüedad demostrable en la explotación y administración de Casinos. Se evaluará sobre los antecedentes presentados por el Oferente correspondientes a los últimos 15 años contados a partir de la fecha de apertura de la presente Licitación, que hayan sido debidamente declarados y acreditados en su propuesta.-

En caso de que el Oferente sea una Unión Transitoria, se evaluará el puntaje de cada empresa que integre la misma y el mayor puntaje de estos será el asignado a la Unión Transitoria.

Máximo cuatro (4) puntos:

Tabla de asignación de puntajes:

Cantidad de años en la actividad	Puntaje
Más de 10 años	4 puntos
Entre 5 y 10 años	2,5 puntos
Menos de 5 años	1 punto
Sin experiencia o no se puede demostrar	0 puntos



a.2- Cantidad de Casinos que Administra/ó u Opera/ó. Se evaluará sobre la experiencia presentada por el Oferente correspondiente a los últimos 15 años contados a partir de la fecha de apertura de la presente Licitación, que hayan sido debidamente declarados y acreditados en su propuesta.

En caso de que el Oferente sea una Unión Transitoria, se evaluará el puntaje de cada empresa que integre la misma y el mayor puntaje de estos será el asignado a la Unión Transitoria.

Máximo cuatro (4) puntos:

Tabla de asignación de puntajes:

Cantidad de casinos	Puntaje
Más de 5	4 puntos
Entre 1 y 5	2,5 puntos
Ninguno o no se puede demostrar	0 puntos

b) Experiencia demostrable en la explotación o provisión de máquinas electrónicas de juegos de azar y su mantenimiento:

Máximo siete (7) puntos:

Los siete (7) puntos de este ítem se dividen en tres sub-ítems:

b.1- Antigüedad demostrable en la explotación o provisión de Máquinas Electrónicas de Juegos de Azar: Se evaluará sobre los antecedentes presentados por el Oferente correspondientes a los últimos 15 años contados a partir de la fecha



de apertura de la presente Licitación, que hayan sido debidamente declarados y acreditados en su propuesta.

En caso de que el Oferente sea una Unión Transitoria, se evaluará el puntaje de cada empresa que integre la misma y el mayor puntaje de estos será el asignado a la Unión Transitoria.

Máximo tres (3) puntos:

Tabla de asignación de puntajes:

Cantidad de años	Puntaje
Más de 10 años	3 puntos
Entre 5 y 10 años	2 puntos
Menos de 5 años	1 punto
Sin experiencia o no se puede demostrar	0 puntos

b.2- Cantidad de Máquinas Electrónicas de Juegos de Azar que explota o provee. Se evaluará sobre la experiencia presentada por el Oferente que haya sido debidamente declarada y acreditada en su propuesta.

En caso de que el Oferente sea una Unión Transitoria, se evaluará el puntaje de cada empresa que integre la misma y el mayor puntaje de estos será el asignado a la Unión Transitoria.

Máximo cuatro (4) puntos:

Tabla de asignación de puntajes:

Cantidad de máquinas electrónicas de juegos de azar	Puntaje



Más de 2000	4 puntos
Entre 1500 y 2000	2 puntos
Ninguna o no se puede demostrar	0 puntos

c) Proyecto de Inversión: total del proyecto, según considere el programa de inversiones a desarrollar hasta la certificación de inicio de las operaciones.

Se evaluará sobre la propuesta de inversión presentada por el Oferente en los proyectos adjuntados; se valorarán la inversión propuesta, resolución arquitectónica, equipamiento lúdico, diseño y confort, como así también los servicios complementarios que se planteen, que otorguen mayor jerarquía y funcionalidad al conjunto.

Los montos de inversiones consignados en las propuestas deberán contar con el respaldo que lo justifiquen y para lo cual se establece:

- Inversiones en obras: se tomarán índices y/o precios publicados por el Ministerio de Infraestructura y Servicios Públicos aprobados por resolución, vigentes a la fecha de la apertura de la presente Licitación.
- Inversiones lúdicas: se deberán acompañar presupuestos de proveedores de equipamientos y material de juego.

Máximo treinta y tres (33) puntos.

Los treinta y tres (33) puntos de éste ítem se dividen en dos sub-ítems:

c.1- Inversión en el Complejo Edificio.



Máximo dieciocho (18) puntos.

Los dieciocho (18) puntos de éste ítem se dividen en dos sub-ítems:

c.1.1- Se evaluará sobre el Monto de la propuesta de inversión presentada por el

Oferente en los proyectos adjuntados, incluyendo inversión en capital de trabajo, inversión del terreno a valor de valuación fiscal, Inversión en construcciones con índices y precios de referencia publicados por el Ministerio de Infraestructura y Servicios Públicos, inversión en Maquinarias y equipo, mobiliario y enseres, exceptuando las máquinas evaluadas como inversión en salas de juegos conforme al inciso c.2,

La Comisión evaluadora tiene la potestad de exigir que el proyecto de construcción cumpla con las características, calidad, funcionalidad y dimensiones de los espacios a construir para el funcionamiento deseado.

Máximo diez (10) puntos:

Tabla de asignación de puntajes:

Monto ofertado a invertir en el complejo edilicio	Puntaje
Monto máximo ofertado	10 puntos
Segundo monto máximo ofertado	6 puntos
Tercer monto máximo ofertado	3 puntos
Cuarto monto máximo ofertado o mayor	0 puntos



c.1.2. Plazo de finalización de las obras: Se evaluará en base al cronograma de realización de las tareas comprometidas presentado por el Oferente. La Comisión de Preadjudicación controlará el avance de las obras conforme al cronograma presentado por el Oferente y determinará las condiciones de finalización de obra que permita el inicio de las operaciones en las salas.

A las ofertas que propongan el menor plazo para la finalización de las obras que permita el inicio de las operaciones en las salas comprendidas se le asignaran ocho (8) puntos:

Tabla de asignación de puntajes:

Plazo de finalización de Obras	Puntaje
Plazo menor al 50% del máximo establecido	8 puntos
Plazo entre 30% y 50% menor al máximo establecido	3 puntos
Plazo menor en hasta un 30% del máximo establecido	0 puntos

c.2. Inversión en las salas de Juegos: Se evaluará sobre el monto y evaluación de prestaciones de la propuesta de inversión presentada por el Oferente con relación al parque de máquinas que pondrá en explotación y a los sistemas de control en línea, de cajas y de fidelización de clientes, ajustados a las normas que se explicitan en el presente pliego, conforme a lo establecido en el artículo 10 del Pliego de Condiciones Particulares. Asimismo, se evaluará el cumplimiento del Sistema a las funcionalidades detalladas en el Reglamento de MEJAAs en los Casinos de la Provincia de Buenos Aires según resolución vigente.

Máximo quince (15) puntos:

Los quince (15) puntos de éste ítem se dividen en dos sub-ítems:

c.2.1 Maquinas: en relación a la cantidad de máquinas de cada caso.



Tabla de asignación de puntajes Máquinas:

Máximo Nueve (9) puntos:

Monto ofertado a invertir en máquinas	Puntaje
Inversión mayor ofertado en Máquinas	9 puntos
Segundo monto máximo de inversión	5 puntos
Tercer monto máximo de inversión ofertado	3 puntos
Cuarto monto máximo ofertado o mayor	0 puntos

c.2.2 - Sistemas

Tabla de asignación de puntajes

Máximo Seis (6) puntos:

Monto ofertado a invertir en las salas de juego	Puntaje
Mayor puntaje de evaluación de prestaciones	6 puntos
Segundo puntaje de evaluación de prestaciones	3 puntos
Tercer puntaje de evaluación de prestaciones	1 puntos
Cuarto puntaje de evaluación de prestaciones	0 puntos



d) Porcentaje cotizado por las prestaciones, objeto de la presente licitación, conforme a lo establecido en el Artículo 6 del Pliego de Condiciones Particulares. Máximo cuarenta y cinco (45) puntos. Se asignará el máximo del puntaje a quien cotice menor porcentaje. Quedará rechazada toda oferta que presente una diferencia mayor a 10 puntos porcentuales respecto de la oferta mínima presentada que cumpliera satisfactoriamente con los requisitos técnicos y económicos detallados.

Tabla de asignación de puntajes:

Porcentaje ofertado	Puntaje
Porcentaje mínimo ofertado	45 puntos
Segundo porcentaje mínimo ofertado	20 puntos
Tercer monto máximo ofertado	10 puntos
Cuarto porcentaje mínimo ofertado o más	0 puntos

e) Evaluación Financiera

Atributos de los estados contables anuales oficiales de cierre de ejercicio económico conforme lo establecido en el artículo 10 del Pliego de Condiciones Particulares.

Se evaluarán los indicadores mencionados a continuación cuyos valores de las fórmulas definidas se extraerán de los rubros correspondientes (activo corriente, pasivo corriente, patrimonio neto, etc.) de los estados contables del último ejercicio económico anual cerrado del Oferente. Para el caso de la evolución de los índices económicos financieros, la evaluación se hará sobre los tres (3) últimos ejercicios económicos del Oferente.



En el caso de que el Oferente sea una Unión Transitoria, se calcularán los indicadores para cada empresa integrante de la misma sobre la base de la información contenida en sus respectivos estados contables y con ellos se determinará para cada indicador el promedio ponderado por el porcentaje de participación de cada empresa en la Unión Transitoria, promedios éstos que serán adoptados como indicadores de la Unión Transitoria.

Puntaje Máximo: siete (7) puntos:

Los siete (7) puntos de este Ítem, se dividen en cinco sub- ítems:

e.1 Relación de endeudamiento (pasivo total dividido patrimonio neto) Puntaje Máximo: un (1) punto. Se asignará el máximo del puntaje a quien presente menor relación de endeudamiento en base a los estados contables presentados del último ejercicio económico anual cerrado del Oferente.

Tabla de asignación de puntajes:

Relación de Endeudamiento	Puntaje
Menor a 0,39	1 punto
Entre 0,40 y 0,59	0,5 puntos
0,60 o más	0 puntos

e.2 Solvencia (Activo total dividido pasivo total). Puntaje Máximo: dos (2) puntos. Se asignará el máximo del puntaje a quien presente mayor relación en base a los estados contables presentados del último ejercicio económico anual cerrado del Oferente.



Tabla de asignación de puntajes:

Índice de Solvencia	Puntaje
1,80 o más	2 puntos
Entre 1,50 y 1,79	1 punto
Menor a 1,50	0 puntos

e.3 Índice de liquidez corriente (activos corrientes dividido pasivos corrientes). Puntaje Máximo: un (1) punto. Se asignará el máximo del puntaje a quien presente mayor relación en base a los estados contables presentados del último ejercicio económico anual cerrado del Oferente.

Tabla de asignación de puntajes:

Índice de liquidez	Puntaje
2,50 o más	1 punto
Entre 1,50 y 2,49	0,5 puntos
Entre 0 y 1,49	0 puntos

e.4 Prueba ácida (Activos Corrientes menos Bienes de Cambio dividido Pasivos Corrientes). Puntaje Máximo un (1) punto. Se asignará el máximo del puntaje a quienes presenten mayor relación en base a los estados contables presentados del último ejercicio económico anual cerrado del Oferente.



Tabla de asignación de puntajes:

Prueba ácida	Puntaje
2 o más	1 punto
Entre 1,00 y 1,99	0,5 puntos
Entre 0 y 0,99	0 puntos

e.5 Evolución económico-financiera: Se evaluará la evolución de los índices económicos - financieros que se indican a continuación, para los estados contables correspondientes a los tres (3) últimos ejercicios económicos del Oferente. Puntaje Máximo dos (2) puntos. Se asignará el máximo del puntaje a quienes presenten un comportamiento creciente de los indicadores.

La evolución de un indicador será creciente o decreciente en el período analizado cuando se verifique que la variación entre cada año y el siguiente ha sido siempre positiva o negativa respectivamente. Si en el período considerado se verificaron variaciones entre cada año y el siguiente, tanto positivas como negativas, se tratará de un caso de evolución fluctuante. En el caso que los indicadores se mantengan significativamente constantes a lo largo del ciclo analizado, es decir que el valor máximo y el mínimo no difieran en más del cinco por ciento (5 %) respecto del valor medio, se considerará la evolución como creciente en el caso de la solvencia, la liquidez corriente, la prueba ácida, y como decreciente en el caso de endeudamiento.

Tabla de asignación de puntajes:



INDICADOR DE EVOLUCIÓN DE:	DEFINIDO COMO:	COMPORTAMIENTO	PUNTAJE
Endeudamiento	Pasivo Total/Patrimonio Neto	DECRECIENTE	0,5 Puntos
		FLUCTUANTE O CRECIENTE	0 Puntos
Solvencia	Activo Total/ Pasivo Total	CRECIENTE	0,5 Puntos
		FLUCTUANTE O DECRECIENTE	0 Puntos
Liquidez Corriente	Activo Corriente/ Pasivo Corriente	CRECIENTE	0,5 Puntos
		FLUCTUANTE O DECRECIENTE	0 Puntos
Prueba Ácida	(Activo Corriente- Bienes de Cambio)/ Pasivo Corriente	CRECIENTE	0,5 Puntos
		FLUCTUANTE O DECRECIENTE	0 Puntos

**EMPATE GENERAL: CRITERIO DE DESEMPATE.** Si como resultado del estudio de las Ofertas surgieran DOS (2) o más que cumplieran satisfactoriamente con los requisitos técnicos y económicos detallados, la pre adjudicación corresponde a la propuesta que ofrezca mayor cantidad de elementos de origen nacional. De subsistir el empate se solicitará a los Oferentes que, por escrito y dentro de los tres (3) días, formulen una mejora de precios.

Las nuevas propuestas que se presenten, son abiertas en el lugar, día y hora establecidos en el requerimiento, labrándose el Acta pertinente.

El silencio del Oferente invitado a desempatar, se entiende como mantenimiento de la propuesta sin modificación.

De mantenerse el empate, se analizará la posibilidad de adjudicar en base a otros criterios, tales como: mayor cantidad de criterios sustentables incorporados a la



oferta, mayor cantidad de elementos de mejor calidad o características diferenciales similares.

Si ninguno de estos criterios resultara de aplicación, la Comisión de Preadjudicación procede al sorteo público de las ofertas empatadas. Para ello debe fijarse día, hora y lugar del sorteo público y notificarse a los Oferentes llamados a desempatar.

### **PLANILLA DE CALIFICACIÓN**



RUBRO	CONCEPTO	PUNTAJE				
a	Experiencia del Oferente en administración y explotación de casinos	8	a-1	Cantidad de años	Más de 10 años	4 puntos
					Entre 5 y 10 años	2,5 puntos
					Menos de 5 años	1 punto
					Sin experiencia o no se puede demostrar	0 puntos
			a-2	Cantidad de casinos	Más de 5 casinos	4 puntos
					Entre 1 y 5 casinos	2,5 puntos
				Ninguno o no se puede demostrar	0 puntos	
b	Experiencia del Oferente en la explotación o provisión de máquinas electrónicas de juegos de azar y su mantenimiento	7	b-1	Cantidad de años	Más de 10 años	3 puntos
					Entre 5 y 10 años	2 puntos
					Menos de 5 años	1 punto
					Sin experiencia o no se puede demostrar	0 puntos
			b-2	Cantidad de máquinas	Más de 2000 máquinas electrónicas de juegos de azar	4 puntos
					Entre 1500 y 2000 máquinas electrónicas de juegos de azar	2 puntos
				Ninguna o no se puede demostrar	0 puntos	
c	Proyecto de Inversión	33	c-1.1	Complejo Edificio	Monto máximo ofertado	10 puntos
					Segundo monto máximo ofertado	6 puntos
					Tercer monto máximo ofertado	3 puntos
					Cuarto monto máximo ofertado o mayor	0 puntos
			c-1.2	Plazo finalización	Plazo menor al 50 % del máximo establecido	8 puntos
					Plazo entre 30% y 50% menor al máximo establecido	3 puntos
					Plazo menor al 30% del máximo establecido	0 puntos
			c-2.1	Máquinas	Inversión mayor ofertado en Máquinas	8 puntos
					Segundo monto máximo de inversión	5 puntos
					Tercer monto máximo de inversión ofertado	3 puntos
					Cuarto monto máximo ofertado o mayor	0 puntos
			c-2.2	Sistemas	Mayor puntaje de evaluación de prestaciones	6 puntos
Segundo puntaje de evaluación de prestaciones	3 puntos					
Tercero puntaje de evaluación de prestaciones	1 puntos					
Cuarto puntaje de evaluación de prestaciones	0 puntos					



RUBRO	CONCEPTO	PUNTAJE					
d	Porcentaje cotizado por las prestaciones, objeto de la presente licitación	45	d	Porcentaje cotizado por las prestaciones	Porcentaje mínimo ofertado	45 puntos	
					Segundo porcentaje mínimo ofertado	20 puntos	
					Tercer monto máximo ofertado	10 puntos	
					Cuarto porcentaje mínimo ofertado o más	0 puntos	
e	Evaluación financiera	7	e-1	Pasivo	Menor a 0,39	1 punto	
				Total/Patrimonio Neto	Entre 0,40 y 0,59	0,5 puntos	
			e-2	Activo Total/ Pasivo Total	0,60 o más	0 puntos	
					1,80 o más	2 puntos	
					Entre 1,50 y 1,79	1 punto	
			e-3	Activo Corriente/ Pasivo	Menor a 1,50	0 puntos	
					2,50 o más	1 punto	
			e-4	(Activo Corriente- Bienes de	Entre 1,50 y 2,49	0,5 puntos	
					Entre 0 y 1,49	0 puntos	
			e-5	(Activo Corriente- Bienes de	2 o más	1 punto	
					Entre 1,00 y 1,99	0,5 puntos	
					Entre 0 y 0,99	0 puntos	
					Pasivo	Evolución Creciente	0,5 Puntos
					Total/Patrimonio Neto	Evolución Fluctuante o Dcreciente	0 Puntos
					Activo Total/ Pasivo Total	Evolución Creciente	0,5 Puntos
					Activo Corriente/ Pasivo	Evolución Fluctuante o Dcreciente	0 Puntos
(Activo Corriente- Bienes de	Evolución Creciente	0,5 Puntos					
	Evolución Fluctuante o Dcreciente	0 Puntos					

## ARTICULO 18°. GARANTÍAS.

### 1.- Las garantías se registrarán de acuerdo a lo siguiente:

a) De mantenimiento de la oferta: los oferentes deberán acompañar, junto al resto de la documentación requerida, una garantía de mantenimiento de oferta equivalente al cinco por ciento (5%) de la suma que signifique el porcentaje de la rentabilidad pretendido como contraprestación, en el primer año de explotación.

A partir del día siguiente de la fecha del acto administrativo de Adjudicación los oferentes no adjudicados deberán retirar las garantías ofrecidas.

b) De Cumplimiento de contrato: el adjudicatario deberá reemplazar, dentro de los diez días de notificado el acto administrativo que aprueba la licitación, la garantía de mantenimiento de oferta por una garantía de cumplimiento de contrato, equivalente al diez por ciento (10%) de la suma que signifique el porcentaje de la rentabilidad



pretendido como contraprestación, en el primer año de explotación. La póliza deberá renovarse anualmente procediendo a reajustarse el monto equivalente al porcentaje solicitado, en relación al año de explotación.

Dicha garantía será liberada a los treinta (30) días de vencido el plazo contractual y bajo la condición de que estuvieren íntegramente satisfechos los deberes y responsabilidades del adjudicatario, incluyendo el plan de transición.

c) Garantías adicionales: sin perjuicio de las garantías exigidas en los incisos anteriores, el INSTITUTO fundado en razones de oportunidad, mérito y conveniencia podrá exigir garantías adicionales de acuerdo a la evolución de la actividad.

## **2.- Falta de constitución de las garantías.**

La falta de constitución de cualquiera de las garantías exigidas o exigibles o de su correspondiente actualización es causal de rechazo de la oferta, impugnación o de resolución del contrato, según el caso.

## **3.- Formas de constitución:**

Salvo los casos en que se indique específicamente el tipo de garantía requerida, las garantías podrán constituirse por alguna de las siguientes formas:

- a) En efectivo, mediante depósito bancario en la cuenta que a tal efecto destine la Tesorería General de la Provincia.
- b) Mediante aval bancario u otra fianza a satisfacción del INSTITUTO, constituyéndose el fiador en deudor solidario, principal pagador, en los términos del artículo 1.591 del Código Civil y Comercial.
- c) Mediante seguro de caución a través de pólizas emitidas por compañías de seguros autorizadas por la Superintendencia de Seguros de la Nación, extendidas a favor del INSTITUTO.



d) Mediante títulos públicos emitidos por la Provincia de Buenos Aires, que deben ser depositados en el Banco de la Provincia de Buenos Aires a la orden del INSTITUTO. El monto se debe calcular tomando la cotización de los títulos al cierre del penúltimo día hábil anterior a la constitución de la garantía, lo que debe ser certificado por las autoridades bancarias al recibir dicho depósito. En caso de liquidación de los valores a que se refiere este inciso, se formulará el cargo por los gastos que ello ocasione. El eventual excedente queda sujeto a las disposiciones que rigen para la devolución de garantías. Los intereses de los títulos pertenecen al propietario y no acrecentarán la garantía.

#### **ARTÍCULO 19°. RESPONSABILIDAD CIVIL.**

19.1. El INSTITUTO estará absolutamente exento de responsabilidad por cualquier daño, cualquiera que sea su motivo, que sufra el adjudicatario, sus dependientes, personal de las distintas actividades, el público y cualquier otra persona, o bienes que resultaren afectados como consecuencia de la correcta prestación de los servicios a cargo del adjudicatario.

19.2. El adjudicatario es el único responsable de la relación entre él y el personal que afecte para llevar a cabo el servicio a que se refiere la convocatoria, así como para dirimir cualquier dificultad o conflicto que pueda surgir entre él y su personal o de su personal entre sí. El adjudicatario asume expresamente dicha responsabilidad en forma íntegra, sin ningún tipo de limitación cuantitativa o temporal.

19.3. El adjudicatario se obliga a constituir seguros de responsabilidad civil frente a terceros por cualquier contingencia motivada por hechos relativos o concernientes a la actividad derivada de la prestación de servicios a su cargo, en cuanto a las cosas o actividades, ya sea por responsabilidad y/o culpa objetiva por riesgos o vicios.

19.4. Será condición indispensable que previo al comienzo de las actividades, se constituyan Seguros y se abonen en su totalidad las pólizas respectivas. En prueba



de su cumplimiento deberán entregarse al INSTITUTO fotocopias certificadas de las pólizas por Escribano Público. En caso de Coaseguros, la Póliza piloto expresará los porcentajes tomados por cada Compañía y el pacto de solidaridad entre éstas. Se presentará certificación correspondiente dejando constancia que las aseguradas privadas no registran deudas exigibles.

19.5. Los seguros se actualizarán periódicamente en la medida suficiente para cubrir los riesgos involucrados.

19.6. Todo incumplimiento causado por falta de prestación del servicio en tiempo y forma, es responsabilidad del adjudicatario quien queda a su exclusivo cargo todo reintegro y/o daño causado.

19.7. El adjudicatario se constituye en único responsable ante reclamos de terceros por derechos de autoría, marcas y/o patentamiento del software, equipamiento o cualquier otro elemento que esté bajo su provisión propia o de terceros, para el cumplimiento del objeto de la presente convocatoria.

19.8. El adjudicatario es responsable exclusivo ante el INSTITUTO, ante los organismos y entidades pertinentes, y ante sus empleados del cumplimiento de las leyes sociales, laborales y previsionales y del pago de toda tasa, contribución o impuesto de cualquier origen o naturaleza por la prestación de servicios a su cargo.

El adjudicatario deberá presentar un seguro contra incendio y todo otro riesgo o deterioro o destrucción de los bienes muebles e inmuebles comprendido en el servicio. A tal fin presentará fotocopia certificada por Escribano Público de las pólizas y del recibo oficial de pago total emitido por la compañía aseguradora. El adjudicatario tendrá un plazo de siete (7) días desde la notificación de la adjudicación para la presentación de los mismos.

## **ARTÍCULO 20º. FISCALIZACIÓN.**



En forma directa o a través de terceros, el INSTITUTO se reserva los derechos para efectuar todos los controles, fiscalizaciones y auditorías necesarias con relación a la implementación, desarrollo, funcionamiento y operatividad de los sistemas objeto de la presente licitación.

El INSTITUTO, por cuenta propia o por designación de tercero, tendrá acceso en forma inmediata y en cualquier momento a toda la documentación y datos que se le soliciten al adjudicatario, como también acceso a todas las oficinas, al sistema y a todas las áreas vinculadas con dicha operatoria y emprendimiento.

#### **ARTÍCULO 21°. INTRANSFERIBILIDAD DE LA ADJUDICACIÓN. MODIFICACIONES SOCIETARIAS- AUTORIZACIÓN PREVIA.**

El contrato es intransferible. Cualquier alteración en la persona o alteración en las responsabilidades del adjudicatario (cambio de uno o más socios, incorporación de nuevos socios, fusiones, transformaciones, escisiones, cambio de componentes del órgano de dirección, derechos reales sobre las acciones del adjudicatario o de la sociedad que lo controle mayoritariamente) deberá ser sometida a la previa aprobación del INSTITUTO, siendo facultad de ésta no aceptar dichas modificaciones o cambios

La omisión de efectuar la solicitud de autorización o la realización de cualquier ardid o engaño destinado a burlar esta condición encubriendo la transmisión de cualquiera de los derechos emergentes de esta autorización, será considerada falta grave, acarreará la rescisión del contrato. El adjudicatario no tendrá derecho en tal supuesto a reclamar indemnización por ninguna causa o especie. El INSTITUTO se reserva el derecho de reclamar a todos aquellos que hayan intervenido en la omisión, ardid o maniobra la indemnización que correspondiere.

#### **ARTICULO 22°: TRASLADO POR RAZONES FUNDADAS Y/O CUESTIONES DE FUERZA MAYOR**



En caso de que, durante la vigencia del plazo licitatorio, el adjudicatario decidiera trasladar la sala de casino a otro inmueble dentro del mismo municipio, por razones fundadas y/o cuestiones de fuerza mayor que así lo obligaran, deberá contar previamente con la conformidad del INSTITUTO.

### **ARTÍCULO 23º. PROPIEDAD INTELECTUAL Y PROTECCIÓN DE MARCAS.**

Es responsabilidad exclusiva y excluyente para con el INSTITUTO el cumplimiento por parte del adjudicatario de las normas relativas a la Ley de Derechos de Autor, Ley de Patentes y las normas aplicables en materia de secretos comerciales o Ley de Confidencialidad, siendo el mismo responsable por la legalidad del producto ofrecido y/o adjudicado, garantizando la total indemnidad al INSTITUTO. En caso de reclamos de terceros por infracción a sus derechos, el adjudicatario será responsable por las demandas judiciales que pudieren establecerse por el uso ilícito de marcas, patentes y/o derechos de autor pertenecientes a terceros.

El INSTITUTO solo autorizará a quien resulte adjudicatario de la presente licitación al uso de las marcas, isotipos, logotipos e isologotipos, exclusivamente en el ámbito de la presente contratación. La presente autorización es indelegable e intransferible y podrá ser revocada unilateralmente por este INSTITUTO sin que ello implique resarcimiento alguno.

Todas las marcas utilizadas y sus logotipos, isotipos e isologotipos son marcas registradas del INSTITUTO, cualquiera otra finalidad, destino o uso, distinto al autorizado en el párrafo anterior, que pretenda hacerse sobre dichas marcas, logos, designaciones y/o frases publicitarias se penarán conforme a la Ley Nacional N° 22.362 y demás normativa aplicable.

### **ARTÍCULO 24º. ACUERDO DE CONFIDENCIALIDAD.**



El INSTITUTO es propietario de la información que genere la prestación del servicio contratado, comprometiéndose el adjudicatario a proteger dicha información, evitando su divulgación, estándole prohibido utilizar la misma, sin la expresa autorización del INSTITUTO. El adjudicatario se abstendrá de usar y revelar la información sobre cuya confidencialidad se previene debiendo suscribir el “Acuerdo de Confidencialidad” que se agrega como Anexo I al presente pliego y que forma parte integrante del mismo.

#### **ARTÍCULO 25°. PROTECCIÓN DE DATOS PERSONALES.**

El adjudicatario será responsable del cumplimiento de la legislación vigente en materia de protección de los datos, archivos, registros de personas a los que tenga acceso en ocasión de la ejecución del servicio contratado.

**ARTICULO 26°. RÉGIMEN DE SANCIONES Y PENALIDADES.** En caso de verificarse incumplimientos del adjudicatario, el INSTITUTO podrá aplicar las siguientes sanciones:

- En caso de incumplimiento del plazo previsto para la finalización de la obra requerida para cada Casino, detallado en el Capítulo III Artículos 18 y 19 de las Especificaciones Técnicas Básicas, el adjudicatario deberá abonar una suma equivalente al costo que el INSTITUTO deba erogar para mantener funcionando las respectivas salas hasta el momento de entrega y puesta en funcionamiento con más una multa diaria por cada día de retraso en la entrega, que se determinará tomando como base el promedio del Net Win de las Máquinas Electrónicas de Juegos de Azar Automatizadas de los Casinos de la Provincia, correspondiente al mes inmediato anterior al incumplimiento, multiplicado por la cantidad de máquinas que estén previstas para la correspondiente Sala.



- Por el incumplimiento en la prestación de los servicios detallados en el Capítulo II, Artículo 1 de las Condiciones Particulares, se aplicará una multa que se determinará tomando como base el costo que asuma el INSTITUTO para cumplir y mantener los servicios más un 20% (veinte por ciento) adicional en concepto de interés punitivo, por cada día de incumplimiento o mora en la regularización del servicio.
- Por el incumplimiento de la renovación de las Máquinas Electrónicas de Juegos de Azar, detallados en el Capítulo III, Artículo 1, de las Condiciones Técnicas, se aplicará una multa diaria que se determinará tomando como base el promedio del Net Win de las Máquinas Electrónicas de Juegos de Azar Automatizadas de los Casinos de la Provincia, correspondiente al mes inmediato anterior al incumplimiento, multiplicado por la cantidad de máquinas que no han sido reemplazadas.
- Para cualquier incumplimiento referido a: La renovación, funcionamiento, mantenimiento y reparación de la totalidad del parque de Máquinas Electrónicas de Juegos de Azar Automatizadas; la implementación, funcionamiento y mantenimiento de un Sistema On Line, la implementación, funcionamiento y mantenimiento de un Sistema de Monitoreo Ambiental; la implementación, funcionamiento y mantenimiento de un Sistema de Movimientos Físico de Valores; y la implementación, funcionamiento, y mantenimiento de un Sistema de Comunicaciones e infraestructura tecnológica, mencionados en el Capítulo II, Artículo 1 de Condiciones Particulares, se aplicará el régimen sancionatorio establecido en el Reglamento de Máquinas Electrónicas de Juegos de Azar Automatizadas habilitadas en los Casinos de la Provincia de Buenos Aires, y sus modificatorias.
- El mecanismo de pago de las sanciones previstas en los incisos precedentes, se hará efectivo a través de un sistema de retenciones de los importes establecidos como multa sobre las recaudaciones mensuales que corresponda abonar al adjudicatario.



## **ARTICULO 27°. EXTINCIÓN DEL CONTRATO:**

27.1. El Contrato se extinguirá por las siguientes causas:

- a) Vencimiento del Plazo y su eventual prórroga.
- b) Por acuerdo mutuo.
- c) Por rescisión por culpa del Adjudicatario.

27.1.a. Vencimiento del Contrato: El Contrato se extinguirá de pleno derecho y sin necesidad de interpelación previa, judicial ni extrajudicial, al producirse el transcurso de su plazo de vencimiento original o su eventual prórroga.

27.1.b. Mutuo Acuerdo: Por acuerdo expreso de las partes a través de instrumento escrito suscrito por sus representantes, con efecto a partir de lo convenido en el mismo.

27.1.c. Rescisión por culpa del Adjudicatario:

- 1) Por no integrar, completar, actualizar o renovar en término los seguros y garantías exigidas, estando intimado formalmente para hacerlo.
- 2) Por realizar cualquier ardid destinado a desviar las apuestas para generar juego clandestino y/o paralelo, ello sin perjuicio de las acciones penales que fueren pertinentes.
- 3) Por no abonar las multas impuestas, encontrándose firmes y estando intimado formalmente para hacerlo.
- 4) Por realizar cualquier actividad lúdica no autorizada por el INSTITUTO o de otra naturaleza que se aparte del objeto de la convocatoria.
- 5) Cuando por razones imputables al Adjudicatario no se cumpla con la obligación de readecuación de las Salas existentes y/ o de provisión de las nuevas Salas a



brindar dentro de los plazos previstos y transcurridos sesenta días de ser intimado por el INSTITUTO.

6) Cuando por razones imputables al Adjudicatario no se cumpla con el cronograma de instalación de reemplazos de las Máquinas Electrónicas de Juegos de Azar luego de transcurridos sesenta días de haber sido intimados al cumplimiento.

27.2. Consecuencias de la Extinción del Contrato:

27.2.a.) Por vencimiento del Plazo y/ o prórroga: El INSTITUTO dispondrá de sesenta (60) días para la restitución de los espacios cedidos en uso.

27.2.b) Mutuo Acuerdo: El INSTITUTO restituirá los espacios cedidos en uso, conforme los términos y condiciones que se estipulen en dicho acuerdo.

27.2.c) Rescisión por culpa del Adjudicatario, por solicitar concurso preventivo o por declaración de quiebra: En el supuesto que el contrato se rescindiere por cualquiera de dichas circunstancias, el Adjudicatario será pasible de abonar los daños y perjuicios ocasionados por la rescisión. Asimismo, la facultad rescisoria con más el derecho a reclamar los daños y perjuicios que la misma ocasionase, incluye el derecho del INSTITUTO de continuar utilizando los espacios cedidos en uso por el adjudicatario, durante el plazo restante del cumplimiento del contrato.

En caso de efectivizarse cualquiera de los supuestos mencionados precedentemente, se deja constancia que el INSTITUTO procederá a retirar la totalidad del equipamiento de su propiedad, conforme lo establece el Capítulo II, Artículo 2 de Condiciones Particulares del presente Pliego.

## **ARTÍCULO 28º. NORMAS APLICABLES.**

La presente licitación se regirá por las normas de los Pliegos de Bases y Condiciones Generales y Particulares que rigen la misma, por las que componen el Régimen de Compras y Contrataciones (Ley N° 13.981 y modificatorias, Decreto 1300/16), por las respuestas y aclaraciones que sobre las mismas se formulen, por



la oferta, por toda la documentación que se incluya en la misma, por el Reglamento de Máquinas Electrónicas de Juegos de Azar Automatizadas que rigen para los Casinos Oficiales de la Provincia y sus modificatorias, y toda aquella reglamentación que se dicte en el futuro y por la adjudicación. Todo esto conformará el marco contractual que regirá las relaciones entre el adjudicatario y el INSTITUTO.

En caso de discordancias entre lo establecido en el Pliego de Condiciones Generales y lo establecido en el Pliego de Condiciones Particulares, prevalecerán las disposiciones insertas en este último.

#### **ARTICULO 29º. JURISDICCIÓN.**

Para la resolución de cualquier conflicto derivado de la presente convocatoria, las partes se someten a la jurisdicción en lo Contencioso Administrativo del Departamento Judicial La Plata, con renuncia a cualquier otro fuero y/o jurisdicción



### CAPITULO III

## PLIEGO DE BASES Y CONDICIONES TÉCNICAS PARA LA CONTRATACION DE BIENES Y SERVICIOS

El adjudicatario tendrá a su cargo la prestación de un servicio integral, que comprende la totalidad de lo requerido en el Capítulo II de Condiciones Particulares, conforme lo estipulado por las normas internas y externas citadas, y aquellas que rigen por aplicación de las distintas reglamentaciones nacionales, provinciales y municipales.

### **ARTICULO 1º: INSTALACIÓN, RENOVACIÓN, MANTENIMIENTO Y REPARACIÓN DEL PARQUE DE MAQUINAS ELECTRÓNICAS DE JUEGOS DE AZAR.**

La instalación, renovación, funcionamiento, mantenimiento y reparación de la totalidad del parque de Máquinas Electrónicas de Juegos de Azar Automatizadas existentes en los Casinos objeto de la presente Licitación, estará sujeta a los requerimientos administrativos contables y técnicos, establecidos en el Reglamento de Máquinas Electrónicas de Juegos de Azar Automatizadas habilitadas en los Casinos de la Provincia de Buenos Aires, y sus modificatorias.

1.1 Al momento de adjudicarse la presente licitación, el adjudicatario deberá proveer las Máquinas electrónicas de Juego de Azar Automatizadas, las que deberán ser nuevas, sin uso, poseer módulo AFT, y cumplir con todo aquello exigido en el Reglamento de Máquinas Electrónicas de Juego de Azar Automatizadas y sus modificatorias.

La cantidad mínima requerida de Máquinas Electrónicas de Juegos de Azar Automatizadas, con relación a cada Casino, deberá ser la siguiente:



Casino Central de Mar del Plata: 813

Casino Anexo III de Mar del Plata (Hotel Hermitage): 276

Casino Miramar: 210

Casino Pinamar: 100

Casino de Tandil: 232

Casino de Monte Hermoso: 90

Casino Tigre: 1582

En caso de requerirse incrementar la cantidad de Máquinas Electrónicas de Juegos de Azar Automatizadas mencionado precedentemente, el adjudicatario deberá contar con la previa conformidad del INSTITUTO.

#### 1.2. Renovación:

Durante el plazo de vigencia del contrato, deberán renovarse las Máquinas Electrónicas de Juego de Azar Automatizadas mencionadas en el Punto 1.1 de este artículo respetando un promedio ponderado de antigüedad máxima de siete (7) años en cada sala, y lo establecido en el Reglamento de máquinas Electrónicas de Juego de Azar Automatizadas y sus modificatorias. .

Al operar el vencimiento del contrato se exigirá la antigüedad prevista en el artículo 2º de las Condiciones Particulares del presente Pliego.

La cantidad requerida para la renovación, será la siguiente:

Casino Central de Mar del Plata: 813

Casino Anexo III de Mar del Plata (Hotel Hermitage): 276

Casino Miramar: 210

Casino Pinamar: 100



Casino de Tandil: 232

Casino de Monte Hermoso: 90

Casino Tigre: 1582

Stock: 300<sup>1</sup>

<sup>1</sup>: Se requerirá al adjudicatario, la provisión de 300 Máquinas Electrónicas de Juegos de Azar Automatizadas, las que formarán parte de un Stock disponible para cada Renglón objeto de la presente licitación, conforme Capítulo II, Artículo 1 de Condiciones Particulares. Dicho Stock, se dividirá proporcionalmente entre cada renglón, resultando así que cada uno, contará con 100 Máquinas Electrónicas de Juegos de Azar Automatizadas, las que se pondrán en funcionamiento con la previa conformidad del INSTITUTO.

1.3. El Adjudicatario tendrá la provisión exclusiva de las Máquinas Electrónicas de Juegos de Azar Automatizadas con relación a los Casinos Oficiales que integran el/los Renglón/es adjudicado/s en la presente Licitación.

## **ARTICULO 2°: IMPLEMENTACIÓN, FUNCIONAMIENTO, Y MANTENIMIENTO DE UN SISTEMA CONTROL ON LINE.**

Implementación, funcionamiento<sup>1</sup> y mantenimiento de un Sistema de Control On Line, que suministre información sobre los contadores y cualquier suceso significativo operado respecto a las Máquinas Electrónicas de Juegos de Azar Automatizadas existentes en los Casinos de la Provincia de Buenos Aires, acorde los contenidos y formato establecidos por la Autoridad de Aplicación en el Reglamento de Máquinas Electrónicas de Juegos de Azar Automatizadas habilitadas en los Casinos de la Provincia de Buenos Aires, y sus modificatorias.

<sup>1</sup>*El funcionamiento implica la correcta operación de acuerdo a las exigencias técnicas y de conformidad a la normativa aplicable.*



### **ARTICULO 3º: IMPLEMENTACIÓN, FUNCIONAMIENTO Y MANTENIMIENTO DE UN SISTEMA DE MONITOREO AMBIENTAL.**

Implementación, funcionamiento<sup>1</sup> y mantenimiento de un Sistema de Monitoreo Ambiental, que permita la visualización de las Máquinas Electrónicas de Juegos de Azar Automatizadas habilitadas en los Casinos de la Provincia de Buenos Aires, acorde los requerimientos administrativos y técnicos, establecidos por la Autoridad de Aplicación en el Reglamento de Máquinas Electrónicas de Juegos de Azar Automatizadas habilitadas en los Casinos de la Provincia de Buenos Aires, y sus modificatorias.

*<sup>1</sup>El funcionamiento implica la correcta operación de acuerdo a las exigencias técnicas y de conformidad a la normativa aplicable.*

### **ARTICULO 4º: IMPLEMENTACIÓN, FUNCIONAMIENTO Y MANTENIMIENTO DE UN SISTEMA DE CONTROL DE MOVIMIENTO FISICO DE VALORES.**

Implementación funcionamiento<sup>1</sup> y mantenimiento de un Sistema encargado de registrar e informar en tiempo real, todos los movimientos físico de valores efectuados en los Casinos de la Provincia de Buenos Aires, como consecuencia del funcionamiento de las Máquinas Electrónicas de Juegos de Azar Automatizadas, acorde los requerimientos administrativos y técnicos, establecidos por la Autoridad de Aplicación en el Reglamento de Máquinas Electrónicas de Juegos de Azar Automatizadas habilitadas en los Casinos de la Provincia de Buenos Aires, y sus modificatorias.

*<sup>1</sup>El funcionamiento implica la correcta operación de acuerdo a las exigencias técnicas y de conformidad a la normativa aplicable.*



#### **ARTICULO 5°: IMPLEMENTACIÓN, FUNCIONAMIENTO Y MANTENIMIENTO DE UN SISTEMA DE COMUNICACIÓN E INFRAESTRUCTURA TECNOLÓGICA.**

Implementación, funcionamiento<sup>1</sup> y mantenimiento de un enlace simétrico, dedicado y permanente para la transmisión de información entre los Casinos de la Provincia de Buenos Aires y la Autoridad de Aplicación, acorde se establece en el Reglamento de Máquinas Electrónicas de Juegos de Azar Automatizadas habilitadas en los Casinos de la Provincia de Buenos Aires, y sus modificatorias.

*<sup>1</sup>El funcionamiento implica la correcta operación de acuerdo a las exigencias técnicas y de conformidad a la normativa aplicable.*

#### **ARTICULO 6°: PROVISIÓN, INSTALACIÓN, CONFIGURACIÓN, FUNCIONAMIENTO, CAPACITACIÓN, MANTENIMIENTO Y RENOVACIÓN DE LAS REDES HARDWARE, SOFTWARE, E INFRAESTRUCTURA TECNOLÓGICA NECESARIA PARA EL FUNCIONAMIENTO DE LOS CASINOS Y SU INTEROPERACIÓN CON EL INSTITUTO.**

La infraestructura tecnológica para el funcionamiento<sup>1</sup> de los Casinos de la Provincia de Buenos Aires y su interoperabilidad con el INSTITUTO deberá incluir todos los elementos necesarios para ejecutar los trabajos y servicios indicados en la presente documentación, sin perjuicio de todos aquéllos que sin estar expresamente indicados fueran necesarios para que la obra y sus instalaciones sean completas conforme a su fin.

*<sup>1</sup>El funcionamiento implica la correcta operación de acuerdo a las exigencias técnicas y de conformidad a la normativa aplicable.*

Requerimientos de infraestructura tecnológica para los Casinos de la Provincia de Buenos Aires



### Casino Central Mar del Plata

INFRAESTRUCTURA DATA ROOM (según cod: ETDC001 según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad / dimensión
Data ROOM (superficie)	5 m2 (cinco metros cuadrados)
Piso Técnico Elevado (superficie)	5 m2
Climatización de Precisión potencia 5 Kw	1 (uno)
Racks para Data Center:	2 (dos).
Monitor LCD 17	1 (uno)
KVM Switch	1 (uno)

CONECTIVIDAD CON INSTITUTO (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cant.	Cód. Anexo Especificaciones Técnicas equipamiento informático
Enlace a Internet simétrico dedicado 10Mbps	1 (uno)	ETCNINT10
Firewall / VPN Casinos Mediano (cluster)	2 (dos)	ETFWCASINOS

69



Switch Layer 3 para trunking 24 bocas 10/100/1000	2 (dos)	ETSWL2PS24GB
---	---------	--------------

## CONECTIVIDAD LAN

CABLEADO ESTRUCTURADO (Ref : ETCECC001 según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad / dimensión
Bocas Voz/Datos Categoría 6 E	170 puestos
Racks murales 10u	8 (ocho)
Rack concentrador 42u	1(uno) (ya contado en Data Room)

ELECRONICA DE RED (según en Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cant.	Cód. Anexo x
Switch L3 core 12 puertos de fibra 1000base-SX SFP con fuente de alimentación redundante	2	ETSWL3CR12PFO
Switch L3 core 24 puertos 10/100/1000 rj45 + 4 x SFP 1000Base-SX con fuente de alimentación redundante	2	ETSWL3CR2PGB



Switch L2 piso 48puertos 10/100/1000 rj45 + 4 x SFP4 1000Base-SX	4	ETSWL2PS48GB
Switch L2 piso 24 puertos 10/100/1000 rj45 + 4 x SFP4 1000Base-SX	4	ETSWL2PS24GB

EQUIPAMIENTO SERVICIOS CENTRALES SERVIDORES (según cod: ETSRVBPRACK en Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad
Servidor bi-procesador rack 128 GB RAM 2tb HD SAS raid2 1	2

#### EQUIPAMIENTO DESKTOP

PC DE ESCRITORIO (Según Cod: ETPCSMLF en Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad
PC – CAJAS Small Factor (ETPCSMLF)	35

IMPRESORAS (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)



Item	Cant.	Cód. Anexo x Especificaciones Técnicas equipamiento informático
IMPRESORA TERMICA	32	ETPRTERM
IMPRESORA LASER DUPLEX RED	5	ETPRTLSDPL

OTROS (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad / dimensión
LECTOR DE TARJETAS RFID USB (ETDRUSB)	32

#### CASINOS ANEXOS

LISTA DE SALAS: Casino Hermitage, Casino Miramar, Casino Pinamar,  
Casino de Tandil, Casino de Monte Hermoso

DATA ROOM (según Cod: ETDC002 Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Requerimiento para cada sala anexa:

Item	Cantidad / dimensión
Data ROOM (superficie)	3,24 M2 (tres metros veinticuatro centímetros)
Piso Técnico Elevado (superficie)	3,24 m2
Climatización de Precisión potencia 3,5 KW	1 (uno)



Racks para Data Center:	1 (uno)
Monitor LCD 17	1 (uno)
KVM Switch	1 (uno)

CONECTIVIDAD CON INSTITUTO (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Requerimiento para cada sala anexa:

Item	Cant.	Cód. Anexo Especificaciones Técnicas equipamiento informático
Enlace a Internet simétrico dedicado 10Mbps	1 (uno)	ETCNINT10
Firewall / VPN Casinos chico (cluster)	2 (dos)	ETFWCASINOSC
Switch Layer 3 para trunking 24 bocas 10/100/1000	2 (dos)	ETSWL2PS24GB

CONECTIVIDAD LAN

CABLEADO ESTRUCTURADO (ETCECC002 según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Requerimiento para cada sala anexa:

Item	Cantidad / dimensión
------	----------------------



Bocas Voz/Datos Categoría 6 E	18 puestos
Racks murales 10u	1

ELECRONICA DE RED (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad / dimensión
Switch L2 piso 24 puertos 10/100/1000 rj45 + 4 x SFP1000Base-SX (ETSWL2PS24GB)	1

#### EQUIPAMIENTO SERVICIOS CENTRALES

SERVIDORES (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad / dimensión
Servidor mono procesador rack 32 GB RAM 1tb HD SAS1raid 1(ETSRVMPRACK)	1

#### EQUIPAMIENTO DESKTOP

PC DE ESCRITORIO (según cod.: ETPCSMLF en Anexo III – Especificaciones Técnicas Equipamiento Informático.)



Item	Cantidad
PC – CAJAS Small Factor	12

IMPRESORAS (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cant.	Cód. Anexo X Especificaciones Técnicas equipamiento informático
IMPRESORA TERMICA	9	ETPRTERM
IMPRESORA LASER DUPLEX RED	2	ETPRTLSDPL

OTROS (según cod : ETRDRUSB en Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cant.
LECTOR DE TARJETAS RFID USB	9

## CASINO TIGRE

INFRAESTRUCTURA DATA ROOM (según cod: ETDC001 Anexo III – Especificaciones Técnicas Equipamiento Informático.)



Item	Cantidad / dimensión
Data ROOM (superficie)	5 m2 (cinco metros cuadrados)
Piso Técnico Elevado (superficie)	5 m2
Climatización de Precisión	1 (uno)
Racks para Data Center:	2 (dos).
Monitor LCD 17	1 (uno)
KVM Switch	1 (uno)

CONECTIVIDAD CON INSTITUTO (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cant.	Cód. Anexo Especificaciones Técnicas equipamiento informático
Enlace a Internet simétrico dedicado 10Mbps	1 (uno)	ETCNINT10
Firewall / VPN Casinos Mediano (cluster)	2 (dos)	ETFWCASINOS
Switch Layer 3 para trunking 24 bocas 10/100/1000	2 (dos)	ETSWL2PS24GB

CONECTIVIDAD LAN

CABLEADO ESTRUCTURADO (según cod: ETCECC001 en Anexo III – Especificaciones Técnicas Equipamiento Informático.)



Item	Cantidad / dimensión
Bocas Voz/Datos Categoría 6 E	170 puestos
Racks murales 10u	8 (ocho)
Rack concentrador 42u	1(uno) (ya contado en Data Room)

ELECRONICA DE RED (según en Anexo III- Especificaciones Técnicas Equipamiento Informático.)

Item	Cant.	Cód. Anexo x Especificaciones Técnicas equipamiento informático
Switch L3 core 12 puertos de fibra 1000base-SX SFP con fuente de alimentación redundante	2	ETSWL3CR12PFO
Switch L3 core 24 puertos 10/100/1000 rj45 + 4 x SFP 1000Base-SX con fuente de alimentación redundante	2	ETSWL3CR2PGB
Switch L2 piso 48puertos 10/100/1000 rj45 + 4 x SFP 1000Base-SX	4	ETSWL2PS48GB
Switch L2 piso 24 puertos 10/100/1000 rj45 + 4 x SFP 1000Base-SX	4	ETSWL2PS24GB

EQUIPAMIENTO SERVICIOS CENTRALES SERVIDORES (según Cod: ETSRVBPRACK en Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad / dimensión
------	----------------------



Servidor bi-procesador rack 128 GB RAM 2tb HD SAS raid2	
1	

## EQUIPAMIENTO DESKTOP

PC DE ESCRITORIO (según cod.: ETPCSMLF en Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad
PC – CAJAS Small Factor	15

IMPRESORAS TERMICAS (según Cod: ETPRTTERM en Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad
IMPRESORA TERMICA – CAJAS (ETPRTTERM)	15

Requerimientos de infraestructura tecnológica Centro de Monitoreo y Control de Salas de Juego del INSTITUTO

PROCESAMIENTO Y ALMACENAMIENTO Upgrade (ETSRVSTO según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cantidad
------	----------



Cajón Blade Cisco UCS (contenedor para instalar los servidores (Hojas))	1
Servidor Blade Cisco UCS (hojas) 2 CPU 256 Gb RAM	12
Pack de discos para EMCVNX4500 para 50 Tbytes de capacidad (discos SSD y SAS – son los más rápidos )	1
Pack de discos para EMCDD2500 para 12 Tbytes de capacidad	1
Software de Gestión de Virtualización VMWare. Licencias para la gestión de toda la plataforma	1

CONECTIVIDAD (según Anexo III – Especificaciones Técnicas Equipamiento Informático.)

Item	Cant.	Cód. Anexo x Especificaciones Técnicas informático equipamiento
Firewall VPN Central	2 (Dos)	ETFWCENTRAL
Enlace a Internet Simétrico dedicado 50 Mbps	1 uno	ETINTSMT50

Los costos de implementación, funcionamiento y mantenimiento del Centro de Control, estarán a cargo del que resulte adjudicatario en cada uno de los renglones previstos en el Artículo 1º del Capítulo II de Condiciones Particulares del presente Pliego.

Cada adjudicatario deberá participar en los costos antes referidos, en forma proporcional a la cantidad de máquinas electrónicas de juegos de azar automatizadas, habilitadas en todos los Casinos de cada renglón.



## **ARTICULO 7°: PROVISION, MANTENIMIENTO Y RENOVACION DE MESAS DE JUEGOS DE PAÑO, INSUMOS Y ACCESORIOS NECESARIOS.**

El adjudicatario deberá proveer la totalidad de los bienes detallados en el presente Artículo. Para efectuar la renovación, el adjudicatario deberá contar con un stock idéntico al provisto inicialmente de la totalidad de los bienes, sin uso, de similares características y calidad. La entrega se coordinará con el INSTITUTO a fin de garantizar el correcto funcionamiento del equipamiento instalado. Agotado dicho stock de renovación, el mantenimiento y la reposición estará a cargo del INSTITUTO.

### **7.1 Mesas de Ruleta Modelo Americana Doble Tablero**

#### **Base:**

- Bases circulares realizadas en maderas terciadas, MDF y multilaminadas con enchapado de madera caoba, 1ª calidad lustrado al poliuretano duro semi mate.
- Sector inferior con aplique laminado oro con soportes al tono.
- Caño posapies de 2" en bronce en sector inferior pulido.
- Detalles cuidados de terminación (lustre, soportes, tapa tornillos, etc.)

#### **Tablero:**

- Base en multilaminado, tablero bajo Ruleta en multilaminado enchapado y lustrado al poliuretano duro semi- mate.
- Posavasos enchapado y lustrado al poliuretano duro semi mate.
- Barandas perimetrales regresadas y tapizadas en cuero de 1ª calidad reforzado de rápido y fácil recambio.



- Tablero porta paño de rápido y fácil recambio.
- Paño sintético 1ª calidad con soporte de algodón, estampado.
- Baranda separadora de Cilindro en PVC.

**Accesorios que complementan cada mesa:**

- 3 Reguladores de altura de Cilindro
- 1 Caja de banca en acrílico con puerta y cerradura de seguridad
- 1 Visor exhibidor de fichas vertical (capacidad 8 piezas) en acrílico
- 1 Protector de Cilindro en acrílico 10mm. de espesor de 84 x 84 x 50cm. con herrajes (4)
  - 1 Tapa de banca en acrílico con cerradura de seguridad
  - 1 Tapa de Cilindro en acrílico
  - 1 Peón marcado
  - 1 Caja Drop box con herrajes, paleta en acrílico
  - 1 Caja de empleados con herrajes
  - 7 Posavasos
  - 7 Ceniceros

**Medidas: 2,90 x 1,60 x 0,85mt.**

**Cilindros para Mesas de Ruleta**

En este sentido solo se requerirán los accesorios que resulten necesarios, para restaurar los que poseen los Casinos en la actualidad o completos, si fuere



necesario, a criterio exclusivo del personal técnico de los Casinos de la provincia, según las siguientes especificaciones técnicas:

- Deberán realizarse totalmente en aluminio especial
- Olla porta eje en aluminio especial refinado línea ERGAL alta resistencia para mecanizado en CNC
- Plato central giratorio en aluminio especial refinado línea ERGAL alta resistencia para mecanizado en CNC
- Aro casillero de bola en aluminio línea ERGAL alta resistencia para mecanizado en CNC confeccionado en una sola pieza otorgando máxima seguridad
- Caja de giro en materiales especiales para alojar rodamientos
- Eje en acero cromo níquel templado
- Torre ornamental confeccionada en materiales especiales diseños personalizados acabado brillante
- Cazuela exterior en maderas especiales torneadas, enchapadas y lustradas, con pinturas de alta resistencia terminación brillante – Cono central iguales características
- Aro superior en maderas especiales torneadas, enchapadas y lustradas, con pinturas de alta resistencia terminación brillante, con pista ante desgaste para desplazamiento de bolilla
- Cinta acrílica porta números enteriza, estampados inalterables
- Diamantes en materiales especiales, refinado diseño, dispuestos uniformemente sobre la pista de giro.
- Calibración y ajuste de todos los elementos para su perfecto funcionamiento
- Medidas para uso profesional en salas de Casinos.



## 7.2 Mesas de Black Jack Doble Tablero para siete (7) asientos

### Base:

- Bases circulares realizadas en 2 sectores con piso en maderas terciadas, MDF y multilaminadas con enchapado de madera caoba, 1ª calidad lustrado al poliuretano duro semi mate.
- Sector inferior con aplique laminado oro con soportes al tono.
- Caño posapies de 2" en bronce en sector inferior pulido.
- Detalles cuidados de terminación (lustre, soportes, tapa tornillos, etc.)

### Tablero:

- Base en multilaminado con posavasos enchapado y lustrado al poliuretano duro semi mate.
- Barandas perimetrales regresadas y tapizadas en cuero de 1ª calidad reforzado de rápido y fácil recambio.
- Tablero porta paño de rápido y fácil recambio.
- Paño sintético 1ª calidad con soporte de algodón, estampado.

### Accesorios que complementan cada mesa:

- 1 Caja de banca con cerradura de seguridad
- 1 Descartero
- 1 Sabot en acrílico negro con cerradura de seguridad en Tapa Superior
- 1 Caja Drop box con herrajes, paleta en acrílico
- 1 Caja de empleados con herrajes



- 6/7 Posavasos
- 6/7 Ceniceros

**Medidas: 2,10 x 1,20 x 0,97mt.**

**Siete (7) banquetas tapizadas por mesa con posapie en bronce pulido**

### **7.3 Mesas de Craps Doble Tablero**

#### **Base:**

- Bases circulares realizadas en maderas terciadas, MDF y multilaminadas con enchapado de madera caoba, 1ª calidad lustrado al poliuretano duro semi mate.
- Sector inferior con aplique laminado oro.
- Detalles cuidados de terminación (lustre, soportes, tapa tornillos, etc.)

#### **Tablero:**

- Cuerpo de mesa enchapado y lustrado al poliuretano duro semi mate.
- Apoya fichas laqueado negro.
- Barandas perimetrales regrosadas y tapizadas en cuero de 1ª calidad reforzado de rápido y fácil recambio.
- Goma rebote de dados al tono
- Espejos laterales
- Paño sintético 1ª calidad con soporte de algodón, estampado.

#### **Accesorios que complementan la mesa:**

- 1 Rastrillo para dados



- 1 Posa dados acrílico
- 2 Indicador on/off
- 1 Caja cubre banca acrílica con cerradura de seguridad
- 1 Caja Drop box con herrajes, paleta en acrílico
- 1 Caja de empleados con herrajes

**Medidas: 4 x 1,40 x 1,05mt.**

#### **7.4 Mesas de Poker Texas Holdem Doble Tablero**

##### **Base:**

- Bases circulares realizadas en maderas terciadas, MDF y multilaminadas con enchapado de madera caoba, 1ª calidad lustrado al poliuretano duro semi mate.
- Sector inferior con aplique laminado oro con soportes al tono.
- Caño posapies de 2" en bronce en sector inferior pulido.
- Detalles cuidados de terminación (lustre, soportes, tapa tornillos, etc.)

##### **Tablero:**

- Base en multi-laminado con posavasos enchapado y lustrado al poliuretano duro semi mate.
- Barandas perimetrales re-grosadas y tapizadas en cuero de 1ª calidad reforzado de rápido y fácil recambio.
- Tablero porta paño de rápido y fácil recambio.
- Paño sintético 1ª calidad con soporte de algodón, estampado.

##### **Accesorios que complementan cada mesa:**



1 Caja de banca metálica con cerradura de seguridad

1 Caja Drop box con herrajes, paleta en acrílico

1 Caja de empleados con herrajes

10 Posavasos

**Medidas: 2,55 x 1,35 x 0,75mt.**

**Diez (10) sillas tapizadas por cada mesa**

#### **7.5 Mesas de Punto y Banca Doble Tablero para Siete (7) asientos**

##### **Base:**

- Bases circulares realizadas en maderas terciadas, MDF y multilaminadas con enchapado de madera caoba, 1ª calidad lustrado al poliuretano duro semi mate.
- Sector inferior con aplique laminado oro.
- Detalles cuidados de terminación (lustre, soportes, tapa tornillos, etc.)

##### **Tablero:**

- Base en multilaminado con posavasos enchapado y lustrado al poliuretano duro semi mate.
- Barandas perimetrales regresadas y tapizadas en cuero de 1ª calidad reforzado de rápido y fácil recambio.
- Tablero porta paño de rápido y fácil recambio.
- Paño sintético 1ª calidad con soporte de algodón, estampado.

##### **Accesorios que complementan cada mesa:**

- 1 Caja de banca acrílica con cierre de seguridad



- 1 Descartero
- 1 Sabot de Acrílico Negro con cierre de seguridad de la Tapa Superior
- 1 Pala
- 1 Caja Drop box con herrajes, paleta en acrílico
- 1 Caja de empleados con herrajes
- 7 Posavasos
- 7 Ceniceros

**Medidas: 2 x 1,50 x 0,75mt.**

**Siete (7) sillas tapizadas por cada mesa**

#### **7.6 Paños de Juegos**

**(Se calcula en base doble por número de mesas a los efectos de tener stock de reposición)**

Paños de Juego de Ruleta

Paños de Juego de Black Jack

Paños de Juego de Poker Central Tres

Paños de Juego de Punto y Banca

Paños de Juego de Craps

**MATERIAL:** 100% Poliéster con soporte de algodón en material sintético no tejido.

**PROCESO DE IMPRESIÓN:** Estampado tipo sublimación.

**COLORES:** a seleccionar por personal técnico de los Casinos provinciales.



### 7.7 Visor –Display- para Mesas de Ruleta

Mensajes informativos de resultados e institucionales

Capacidad de recolección de datos

Doble pantalla (visualización anverso y reverso)

Terminación oro/plata

**NOTA:** Las presentes especificaciones y condiciones técnicas, no son condicionantes de soluciones superiores que se evaluarán por personal técnico operativo de los Casinos provinciales. Del mismo modo, los modelos de mesas quedarán sujetos a la aprobación de este personal.

### **ARTICULO 8º: PROVISIÓN Y RENOVACION DE CONTADORAS, CLASIFICADORAS DE BILLETES Y TICKETS Y DETECTORAS DE BILLETES FALSOS.**

El adjudicatario deberá proveer todos los bienes detallados en el presente artículo. Para efectuar la renovación, el adjudicatario deberá contar con un stock idéntico al provisto inicialmente de la totalidad de los bienes, sin uso, de similares características y calidad. La entrega se coordinará con el INSTITUTO a fin de garantizar el correcto funcionamiento del equipamiento instalado. Agotado dicho stock de renovación, el mantenimiento y la reposición estará a cargo del INSTITUTO.

8.1. Provisión, mantenimiento y renovación de Máquinas GLORY GFS 120 Contadoras y Clasificadoras de billetes, con dos (2) bolsillos, o similar de igual o mejor prestación.

8.2. Provisión y renovación Máquinas GLORY GFB 801 Contadoras de billetes para Cajas o Escritorios, o similar de igual o mejor prestación.



8.3. Provisión y renovación de Máquinas NUMERON D Contadora y Clasificadora con tres (3) bolsillos, o similar de igual o mejor prestación.

8.4. Provisión y renovación de Máquinas MULTISCAN MT 31 R procesadora-verificadora de documentación con códigos de barra, o similar de igual o mejor prestación.

8.5. Provisión y renovación de Lámparas Detectoras de Billetes Falsos, unidades equipadas con luz negra y blanca para Cajas o Escritorios.

La cantidad requerida de máquinas, será detallada en el Apartado correspondiente a cada uno de los Casinos.

#### **ARTICULO 9°. PROVISION, FUNCIONAMIENTO, CAPACITACIÓN Y RENOVACION DE SISTEMAS DE CONTROL POR VIDEO.**

Provisión, instalación, configuración, funcionamiento, capacitación y mantenimiento de un Circuito Cerrado de Televisión (o Sistema CCTV), para todos los Casinos alcanzados por la presente licitación.

El adjudicatario deberá proveer todos los elementos necesarios para ejecutar los trabajos y servicios indicados en el presente artículo, sin perjuicio de todos aquellos que sin estar expresamente indicados fueran necesarios para que la obra y sus instalaciones sean completas conforme a su fin.

Para efectuar la renovación, el adjudicatario deberá contar con un stock idéntico al provisto inicialmente de la totalidad de los bienes, sin uso, de similares características y calidad. La entrega será a coordinar con el INSTITUTO, a fin de garantizar el correcto funcionamiento del equipamiento instalado. Agotado dicho stock de renovación, el mantenimiento y la reposición estará a cargo del INSTITUTO.

#### **Sobre el Equipamiento**



El equipamiento ofrecido debe ser de marca y modelo reconocidos, los mismos deben tener antecedentes de instalaciones exitosas en obras con características similares a la que se esta licitando en este pliego.

El equipamiento ofrecido debe contar con canales de comercialización ajenos al oferente.

Los equipos ofrecidos deben ser aptos para operar en el entorno en el cual serán instalados cumpliendo las especificaciones que se detallan a continuación:

- Frecuencia de línea 50Hz.
- Compatible con modulación PAL 50Hz.
- Rango de temperatura de trabajo: -10° C a 50° c.
- Regulaciones de proteccion UL, FCC Class A, CE o S-Mark, antivandálicas IP56 o IK 10, estanqueidad IP66

En el caso en el cual los equipos ofertados no cumplan con algunas de las especificaciones y certificaciones solicitadas, se aceptaran las propuestas técnicas superiores que se adecuen a lo solicitado.

Las hojas de datos presentadas en la propuesta para documentar el cumplimiento de las especificaciones y certificaciones deben ser las que él fabricante tiene publicada en su pagina web oficial. No se aceptaran otras hojas de datos alternativas.

### **Sobre las licencias**

El sistema debe entregarse con todas las licencias de software necesarias incluidas dentro de la propuesta. Deben contemplarse también dentro de la misma, las licencias correspondientes al software que se instale sobre equipamiento existente.

### **Descripción general de la obra.**



Se requiere para esta licitación Sistema de CCTV para el control Interno y externo que incluyan, en la parte interna, Salas de Juegos, Tesoro, Cajas de Atención al público, Pasillos internos, Puertas de Ingreso/Egreso de Público y/o Proveedores y en la parte externa Puertas de Ingreso/Egreso de Público, Personal y/o Proveedores, periferia general del establecimiento con cobertura total de sus alrededores y toda zona de interés.

Todas las instalaciones externas deben tener características anti-vandálicas.

El objeto del sistema de CCTV debe registrar:

- Las mesas de Juegos, con nitidez total de los valores expuestos que garanticen la observación de su cuantía por color, tipo y valor. Sean Fichas o Efectivo.
- En Mesas de Juego y en Maquinas, que se puedan observar los rostros de las personas del público y de los empleados que circulan por las mismas, con claridad necesaria para su identificación.
- La observación general continua de la totalidad de las salas de juego, mediante la instalación de Cámaras Panorámicas.
- Que a los efectos operativos el movimiento de las Cámaras (Domas), se pueda realizar a través de los joysticks con velocidad necesaria que permita el seguimiento y desplazamiento de una/s persona/s que se encuentren en movimiento en cualquier dirección y velocidad en tiempo real.
- En las Cajas que permita la observación de los valores en cuantía por color, tipo y valor. Sean Fichas o Efectivo y/o Tickets de canje por Efectivo; que se observen los movimientos internos del empleado y del lado externo del público y/o empleados.
- En los tesoros de Fichas y Efectivo, que permita la observación del ingreso a las bóvedas y/o cajas fuertes e internas dentro de ellas y de las



Operaciones que se realicen en el ámbito de los Tesoros con visión de los valores que se cuantifiquen y los displays de las Contadoras de Billetes.

- En los pasillos internos, Puertas de Ingreso/Egreso de Público, Personal y/o Proveedores, que se pueda observar con nitidez los rostros y vestimentas de las personas que circulan por los mismos de manera tal que se observe el ingreso, como el egreso.
- Con las Cámaras Externas, que su visión sea Día/Noche, con infrarrojos y/o sistemas que permitan la visión con un mínimo de luz ambiente, que permitan observar con nitidez los rostros y vestimentas de las personas.

El almacenamiento de discos de cada NVR, debe ser calculado para que las cámaras se graben en calidad de HD a 15ips y debe retener las grabaciones de las mismas por un mínimo de veintiún (21) días corridos durante las 24 hs con el códec H.264.

Deberán entregarse con la totalidad de las tareas de configuración y puesta en marcha de todo el equipamiento que provea incluyendo rótulos, configuraciones, mapas, etc.

Para la totalidad de las instalaciones se deben considerar las reglas del buen arte.

Se requiere también para esta licitación el arreglo integral, con materiales de repuesto, y la eventual reinstalación, en caso de que el proyecto así lo establezca, del equipamiento existente en cada Casino comprendido en la presente licitación y que se encuentre en condiciones técnicas de uso.

Para el movimiento de las cámaras domo analógicas existentes se debe contemplar la reinstalación de los traductores de código que se encuentren operativos, de modo tal de simplificar el control de dichas cámaras.

El cableado de las cámaras y los domos analógicos que deban reinstalarse, de acuerdo a las pautas de proyecto, debe ser nuevo utilizando para ello cables del tipo:



Para el video: RG-59/U (de cobre de cobertura del 98%) o similar.

Para datos RS-422: Belden 9729 o similar.

Para datos Sensornet: Belden 8442 o similar.

Para datos Manchester: Belden 8760 o similar.

### **Capacitación.**

El oferente deberá capacitar al personal designado por el INSTITUTO para las tareas de Operador y Administrador, indicando claramente cuales son las bondades y las limitaciones del sistema provisto.

Junto con la capacitación se deberán entregar manuales en castellano que documenten los contenidos de los cursos dictados, con el objeto de que los mismos sirvan de material de consulta tanto para los operadores, como así también, para los administradores del sistema.

La capacitación debe comprender la utilización del sistema tanto desde el VMS, como así también, desde el NVR.

Junto con la bibliografía referente a los cursos, se deben entregar todos los manuales, software, licencias y claves de los sistemas instalados al personal designado por el INSTITUTO.

### **Alimentación de 220 VAC.**

Personal de Mantenimiento de los Casinos, determinarán el punto desde el cual debe ser tomada la alimentación eléctrica de cada sitio.

La alimentación eléctrica debe ser tomada de forma tal, que no interfiera con el normal funcionamiento de la instalación existente, para lo cual, se deberá instalar una térmica y un disyuntor en el punto en el que se toma la energía.



Si en el punto de toma existe un tablero, se puede incluir la térmica en dicho tablero. Si en el punto de toma de energía eléctrica no existe un tablero, se debe instalar uno con llave.

En todos los casos, tanto la térmica como el disyuntor deben estar identificados con la leyenda "CCTV NO APAGAR".

La línea de alimentación debe ser única e independiente para los equipos de CCTV, debiéndose conectar en forma directa al Tablero principal de alimentación de cada Casino.

#### **Especificación de las canalizaciones.**

En el exterior protegida por caño galvanizado.

No se admitirá, tendidos aéreos no cables a la vista.

Toda la canalización de exterior debe ser anti-vandálica.

Todo el cableado en el interior debe estar protegido por caño y/o bandeja.

Por cuestiones de flexibilidad en la reubicación de las cámaras, se aceptará que los últimos 10m de cable antes de llegar a la cámara sean tendidos si cañería de protección.

En todos los casos la canalización debe ser dimensionada de modo tal que la sección neta ocupada por el cableado no exceda el 30% de la sección libre de la canalización.

#### **Especificaciones de la UPS.**

UPS de primera marca, con placa de red.

Autonomía mínima para alimentar los equipos instalados de 30 minutos.

Baterías plomo-acido de libre mantenimiento con electrolito suspendido

Forma de onda de salida: Senoidal



Compatible con protocolos de APC.

Soporte de monitoreo y gestión vía Ethernet.

### **Componentes y Especificaciones del Sistema de gestión centralizada.**

#### **Componentes:**

- a. Una (1) Plataforma VMS (Sistema de Gestión de Video Victor ó similar)
- b. un sistema VMS para monitorear mediante operadores con 1 cliente por operador. La cantidad de clientes se determina a razón de un (1) operador cada 100 cámaras instaladas.
- c. El sistema debe incluir las licencias necesarias de Victor Agent ó similar, mas una (1) licencia de Victor Command Center y tantas Licencias de Cliente Unificado Víctor ó similar como sean necesarias.
- d. Agregar una (1) licencia por operador externo al cctv.
- e. Un (1) Server para el Command Center Site Server (Servidor del Centro de comando).
- f. Tantas PC con las salidas de video necesarias y licencias Víctor Agent ó similar, como operadores se determinen. La cantidad de éstos se determina a razón de un (1) operador cada 100 cámaras instaladas.
- g. Una notebook ó PC i7 para la estación de edición.

#### **Especificaciones Técnicas:**

Deberá ser un sistema centralizado que permita políticas de utilización, permitiendo crear distintos perfiles de usuario con diferentes permisos sobre las cámaras y el registro filmico de las mismas.

Debe poseer una base de datos centralizada para almacenar el registro de video correspondiente a eventos destinados a utilizarse como prueba filmica.



Debe permitir la administración centralizada de las configuraciones de todos los NVR correspondiente al sistema.

Debe poder transcodificar el streaming de video de modo tal que permita el monitoreo remoto desde redes con bajo ancho de banda.

Debe poseer una base de datos centralizada con el registro de actividad de todos los NVR's del sistema.

Debe sincronizar la fecha y el horario de todos los dispositivos que componen el sistema.

Debe permitir el acceso para monitorear desde Internet estableciendo una conexión segura con el sistema.

Debe proveerse el Hardware necesario para que el sistema pueda contar con las prestaciones mencionadas en este pliego.

Debe contar con interfaz de usuario en idioma español.

Debe permitir gestionar de forma centralizada tanto el video en vivo como así tambien las grabaciones contenidas en los NVR.

Debe contemplar que cada cliente del sistema pueda gestionar múltiples monitores desde una misma estación de trabajo.

Debe tener la función de matriz virtual dando la posibilidad de llamar a las cámaras mediante números únicos asignados independientemente de las direcciones IP de las mismas y de la grabadora a la cual se encuentren conectadas.

Debe tener una función que permita la recuperación rápida de una cantidad de tiempo predefinida de las grabaciones más recientes de la cámara que se este visualizando en vivo.

Debe permitir búsqueda de video inteligentes, permitiendo la aplicación de filtros sobre las imágenes grabadas.



Debe contar con distintas opciones de software cliente para el control, visualización y reproducción de imágenes de toda la instalación, con la posibilidad de definir múltiples perfiles de usuario.

Debe contar con distintas matrices de visualización personalizables con mínimo de sesenta y cuatro cámaras simultáneas sobre cuatro monitores.

Configuración de “Tours” de visualización.

Debe permitir el control de play/pausa de al menos 16x de la velocidad normal.

Debe permitir la reproducción de múltiples cámaras de manera simultánea y sincronizada.

Debe contar opciones de PTZ manual, posiciones pre-configuradas y posicionamiento automático como acción de un evento.

Debe poder operarse mediante teclado y Mouse o desde un joystick.

Debe contar con notificaciones para los usuarios sobre eventos y detección de movimiento por sonido e email.

Debe contar con la capacidad de exportar video para ser utilizado como evidencia en formato propietario inalterable.

Debe contar con la capacidad de exportar video en formatos estándar para permitir su edición y compaginación.

Deberá proveer acceso directo e instantáneo al video relacionado a las distintas alarmas que hayan sido configuradas.

Debe proveerse el Hardware necesario para los puestos de visualización en cada estación y en los sitios centrales. El hardware deberá soportar las especificaciones requeridas y la posibilidad de gestionar múltiples monitores por puesto de trabajo.

### **Especificaciones del Reproductor de Video en formato propietario**



El reproductor off-line deberá permitir la reproducción del video de múltiples cámaras de manera simultánea y sincronizada.

Debe permitir la reproducción del video extraído de los NVR en formato propietario a fines que el mismo sirva como prueba fílmica ante la justicia.

Grabadoras NVR modelo VideoEdge ó similar

El número de grabadoras necesarias en cada Casino, se establecerá de acuerdo a la cantidad de cámaras a instalar.

Debe tener marca de agua.

Debe ser un producto de primera marca montado en una línea de producción.

Debe cumplir como mínimo, con el requerimiento solicitado en el detalle de la especificación técnica de este pliego. Debe ser un producto confiable, con antecedentes de instalaciones exitosas comprobables.

La documentación del equipo, tanto hojas de datos como la totalidad de los manuales, deben estar disponibles en el sitio web del fabricante.

Gabinete de 2U apto para el montaje en rack de 19".

Fuente de alimentación redundante.

Debe soportar almacenamiento en Raid 5, Raid 6 o Raid 10 de hasta 90 TB.

Soporte de cliente.

Debe sincronizar el horario con un NTP Server común para todos los NVR's de la red.

Debe permitir configuraciones tipo failover, para que otro equipo comience a grabar las cámaras ante la caída de un NVR.

Debe permitir configuraciones redundantes de forma tal que la grabación del video de las cámaras, se pueda efectuar en dos sitios diferentes de forma simultánea.



Soporte de grabación en resoluciones de CIF, 2 CIF, 4 CIF, HD720, Full HD 1080.

Soporte de programación por franjas horarias que contemple feriados.

Debe ser totalmente compatible con las cámaras y encoders ofertados, de modo tal que el alta de los mismos se efectúe de manera casi automática y se pueden configurar las cámaras desde el NVR sin necesidad de ingresar al webserver de configuración de las mismas.

El almacenamiento en disco se debe calcular para que mantenga la guarda de las imágenes durante veintiún (21) días configurando el sistema para que la grabación se efectúe en calidad HD a 15 ips las 24 hs del día los 365 días del año, utilizando la compresión de video permitida por el algoritmo H.264.

Soporte de análisis de video para generar alarmas cuando:

- Alguien viole un perímetro.
- Alguien ingrese a una zona restringida.
- Objeto ausente para detección de hurtos.

#### **Disco rígido para streaming – Especificaciones básicas.**

- Descripción de producto: WD 2.5" ITB SATA 5KRPM 16MB 9.5MM 24x7
- Aplicación: Almacenamiento de video
- Generación: AV25
- Factor de forma: 2.5 INCH
- Interface: SATA
- Soporte operación 24x7: Si
- Transferencia de datos: 3GB/S



- Velocidad de rotación: 5400RPM
- Memoria Cache: 16MB
- Tiempo de búsqueda promedio: 12.0MS
- Temperatura de operación: 0° C – 60° C
- MTBF: 1,000,000 Hours
- RoHS Status: Si
- Cámaras IP fijas de 2 MP ó superior (con gabinete anti-vandálico)
- Cámara tipo IP
- Triple streaming.
- TWDR (rango dinámico extendido)
- Mínima iluminación (Color: 0.04 lux / B&W: 0.002 lux / IR: 0.0 lux)
- Lente varifocal (según la necesidad)
- Autofocus
- Gabinete tipo mini-domo anti-vandálico IK10.
- Accesorios de montaje en techo / Pared / columna según corresponda.
- Alimentación 24 VAC, 12 VAC, PoE IEEE 802.3af Class 3
- H.264
- ONVIF.
- Cámaras IP móviles (Domos) de 2 MP, 30 X, PTZ
- Cámara tipo IP



- TWDR (rango dinámico extendido)
- Mínima iluminación (Color:0.2 lux / B&W:0.04 lux)
- Lente varifocal motorizado 30X 63.4° (wide); 2.3° (tele).
- Autofocus.
- Accesorios de montaje en techo / Pared / Columna.
- Alimentación 24 VAC, PoE + IEEE 802.3af Class 4.
- H.264
- ONVIF

Cableado y Componentes de Instalación de red.

Equipos para conectar Cámaras y Domos de interior:

Switch de conexasión nivel 1

Especificaciones:

- Switch de primera marca
- Switch administrable capa 2
- 48 puertos 10/100/1000
- 4 puertos UPLINK SFP
- 1 módulo GBIC Gigabit Ethernet para F.O.
- 24 Puertos de hasta 30W PoE+ (IEEE 802.3at) o 48 puertos de hasta 15.4W PoE(IEEE 802.3at)
- Potencia total aplicable a PoER: 740 W



- Soporte de calidad de servicio QoS
- Soporte de hasta 256 VLAN
- Capacidad de Forwarding: 88Gbps
- Capacidad de conmutación: 176 Ggps.
- MTU: 9198 Bytes.
- Soporte de protocolos:
  1. Port Aggregation Protocol (PAgP)
  2. VLAN Transfer Protocol (VTP)
  3. Resilient Ethernet Protocol (REP)
  4. Dynamic Trunking Protocol (DTP)

Conexión de las grabadoras NVR's de los clientes y las cámaras.

Switch de conexionado nivel 2

Especificaciones:

- Switch de primera marca
- Switch administrable capa 3
- 12 puertos SFP
- 8 módulos GBIC Gigabit Ethernet para F.O.
- Soporte de calidad de servicio QoS.
- Soporte de hasta 1005 VLAN simultaneas



- Fuente de alimentación redundante
- Memoria DRAM 512 MB
- Memoria Flash 128 MB
- Puertos de consola
- Interface de almacenamiento USB (Type-A) for external flash
- Soporte de protocolos:
  1. Port Aggregation Protocol (PAgP)
  2. VLAN Transfer Protocol (VTP)
  3. Resilient Ethernet Protocol (REP)
  4. Dynamic Trunking Protocol (DTP)

Switch de conexasión nivel 3

Especificaciones:

- Switch de primera marca
- Switch administrable capa 3
- 48 puertos 10/100/1000
- Soporte de calidad de servicio QoS.
- Soporte de hasta 1005 VLAN simultaneas
- Fuente de alimentación redundante
- Memoria DRAM 256 MB
- Memoria Flash 64 MB



- Puertos de consola
- Interface de almacenamiento USB (Type-A) for external flash
- Soporte de protocolos:
  1. Port Aggregation Protocol (PAgP)
  2. VLAN Transfer Protocol (VTP)
  3. Resilient Ethernet Protocol (REP)
  4. Dynamic Trunking Protocol (DTP)

### **Especificaciones de la fibra óptica**

Los switches del apartado anterior se deberán poder conectar a través de fibra óptica. La F.O. para interconectar los switch debe ser del tipo adecuado para los módulos GBIC elegidos. Indefectiblemente de cuatro (4) pelos anti-roedor y se deberá utilizar un tendido de F.O. por cada switch de borde.

La fibra se tenderá en estrella desde el rack central donde se el switch de core formado por dos switch stackeados hasta uno de los rack de pared donde irán instalados los switch de borde.

La fibra óptica debe terminar:

- En el nodo central, en 2 patcheras de 19" conectadas y amuradas al rack donde se encuentren los switch de core stackeados.
- En cada extremo del lado de los switch de borde, en una patchera de 19" amurada dentro del rack de pared.

La fibra óptica debe ser conectada mediante método pigtail empalmados por fusión.



Las pruebas se realizarán mediante OTDR para asegurar el estado tanto del empalme como de los conectores desde donde se realizan las pruebas.

Para conectar la bandeja y los equipos (switch o transceiver) se utilizarán patchcords del tipo que corresponda.

Todos los elementos utilizados para la obra deben ser productos comerciales de primera marca, desarrolladas para utilizar en obras de F.O.

no se aceptarán patcheras, cassette, bandejas, organizadores, soportes, o cualquier tipo de elemento artesanal.

### **Cableado Ethernet para las cámaras**

Cable de primera marca Categoría 6 (se solicitará certificación cat 6 del cableado)

Todos los accesorios, patcheras y conectores deben ser de primera marca.

Para simplificar la instalación y la futura reubicación de las cámaras se aceptará que el cableado de las mismas se realice con un cableado de un tramo sin cortes ni empalmes de ningún tipo desde la cámara hasta el switch utilizando un RJ-45 macho en caga punta (no se requerirá patchera en los Racks de pared no rosetas junto a las cámaras, pero se exigirá que todos los cables de red correspondientes a las cámaras, se encuentren rotulados con el mismo código en ambas puntas.)

### **Cableado de los NVR's server y clientes de red**

Cable de primera marca

Todos los accesorios, patcheras y conectores deben ser de primera marca.

Categoría 6 (se solicitará certificación cat6 del cableado)

Debido a que los cableados de red entre switch y los NVR se realizará dentro de los racks no se requerirá la utilización de patcheras para estas conexiones. Solo se solicitará la utilización de patcheras y rosetas para los puestos de red que se en instalen fuera del rack.



## Rack de pared

Todos los switch de cámara deben ir protegidos por rack de pared.

La alimentación eléctrica de los Rack de pared debe estar centralizada en un tablero en la sala de Racks principal, en donde exista una térmica independiente para cada rack de pared.

Características del Rack de pared

- Rack de 19" metálico
- 9U x 500 (o superior, debe poder contener todo el equipamiento con la puerta cerrada)
- Puerta de vidrio con llave.
- Cooler de techo.

Dentro de cada rack de pared debe ir instalado:

- Patchera de F.O.
- Switch de borde con puertos PoE.
- Un organizador para proteger los patchcord de F.O.
- Un organizador para contener la punta del cableado de las cámaras.
- Un canal de tensión con térmicas

Rack de NVR's

Un (1) Rack de 19"

- 40U x 1000
- Sin puertas.



- Dos (2) canales de tensión con térmica

Rack para Victor Agent Site Server y equipamiento de red

Un (1) Rack de 19"

- 40U x 1000
- Sin puertas.
- Dos (2) canales de tensión con térmica
- Dos (2) organizadores.

#### **Aire acondicionado para sala de rack's**

La Sala de rack's deberá tener una temperatura estable de 18° C para protección de los equipos.

(Se deberá realizar el cálculo de frigorías en función de la carga térmica de los equipos propuestos)

Teclado con Joystick para integrar con cliente de video

Teclado con joystick para operar matriz virtual y cámaras domo y PTZ

El teclado debe integrarse con el software de monitoreo para agilizar las funcionalidades de del software.

PC para aplicación Server (Servidor)

- Factor de forma 2U
- Procesador 2x Intel Xeon E5 o superior
- Sistema operativo Windows Server 2012R2 o superior



- Memoria RAM 32 GB (8 GB RDIMM x 4)
- Adaptador gráfico onboard
- Discos rígidos 6 x 3.5" hot-plug de 600GB en Raid 10
- Ethernet 1GbE

#### PC para Victor Agent

- Procesador Intel Xeon E3 2.80Ghz o superior
- Sistema operativo Windows 7 Professional 64-Bit o superior
- Memoria 16 GB (2 x 8 GB)
- Disco rígido de 1TB
- Adaptador gráfico NVIDIA Quadro K620 (para cuatro monitores) o superior
- Interface de red 1Gb Ethernet
- Dimensiones (W x H x D) 17.5cm x 36.0 cm x 43.5cm
- Grabadora de DVD
- Cantidad de monitores soportados simultáneamente: 4

#### PC de operador Cliente unificado Victor

- Procesador Intel Xeon E3 2.80Ghz o superior
- Sistema operativo Windows 7 Professional 64-Bit o superior
- Memoria 16 GB (2 x 8 GB)
- Disco rígido de 1TB
- Adaptador gráfico NVIDIA Quadro K620 (para cuatro monitores) o superior



- Interface de red 1Gb Ethernet
- Dimensiones (W x H x D) 17.5cm x 36.0 cm x 43.5cm
- Grabadora de DVD
- Cantidad de monitores soportados simultáneamente: 4

PC de Edición:

Notebook de escritorio

- Procesador Intel i7 de 4ta generación o superior
- 16GB de RAM
- Disco rígido de 1TB
- Monitor de Full HD de 17"
- 

Monitores Led Color Full HD de 32"

El equipo deberá encontrarse preparado para que se instale una VPN, con el equipamiento y el ancho de banda necesario, que podrá ser contratado a una firma proveedora debidamente homologada por los organismos controladores.-

### **Lugar físico a desarrollarse el Centro de Monitoreo**

En la misma se deberá diseñar en forma independiente la Sala de Control con una pared plana y lindante a ésta, una Sala de Rack's independiente con Aire Acondicionado, construida con material transparente que permitan la observación de los equipos desde fuera.

La totalidad de la Superficie de la Sala de Operadores y la sala de Rack's deberá realizarse con Piso Técnico a los efectos de facilitar el tendido de cableado y las tareas de mantenimiento.-

**NOTA 1:**

- Para el desarrollo del presente documento se utilizó el Sistema Víctor de American Dynamics de Tyco (debido a que la marca posee compatibilidad con el equipamiento existente)

Opcionales sugeridos:

- PELCO – Plataforma ENDURA
- NICE – Plataforma de similar o superior performance

**NOTA 2:**

- Las plataformas que no mantengan compatibilidad con el equipamiento existente, deberán agregar DVR's, Encoders, Espacio de almacenamiento, conversores de protocolo y todo lo que sea necesario, para compatibilizar con el equipamiento analógico existente sin perder performance, calidad o capacidad de almacenamiento de video.

**Descripción general del servicio de Mantenimiento**

Se requiere servicio de mantenimiento preventivo y correctivo para los sistemas de CCTV, en la totalidad de las instalaciones de los Casinos alcanzados por la presente licitación.

El mantenimiento preventivo debe brindarse con la frecuencia especificada en el Anexo A. El proveedor del servicio debe contar con la cantidad suficientes de técnicos que acrediten los conocimientos necesarios para cumplir con los requerimientos de esta contratación.

Todas las labores realizadas en la rutina de mantenimiento preventivo, deben quedar documentadas en planillas electrónicas en formato .xls, las cuales deben ser entregadas mensualmente vía e-mail a una dirección de correo electrónico indicada por el INSTITUTO.



El mantenimiento correctivo debe brindarse incluyendo servicio de desinstalación y retiro del material en falla, instalación de equipo muleto (de reemplazo) con las mismas características para no afectar el servicio, reparación del material dañado, repuestos y reinstalación del material reparado.

El prestador de servicio debe atender las necesidades de mantenimiento correctivos derivadas de sus propias rutinas de mantenimiento preventivo, como así también las solicitudes de mantenimiento correctivos provenientes de las áreas designadas por el INSTITUTO.

Por cada equipo, que requiera mantenimiento correctivo, el prestador del servicio debe generar y mantener una ficha de historial, en la que quede documentado el momento en que el equipo sale de servicio, el muleto que lo reemplazó, el detalle de la reparación, el momento en que el equipo entra nuevamente en servicio en su defecto, el momento en el cual el prestador del servicio declara al equipo irreparable.

Esta ficha deberá entregarse vía e-mail a una dirección de correo electrónico indicada por el INSTITUTO, cada vez que el equipo salga de servicio, vuelva a entrar en servicio o sea declarado irreparable.

El proveedor, debe poner operativo el sistema de CCTV al 100 % en el plazo indicado en el anexo A, Este lapso de tiempo se contará a partir de la fecha de iniciación del servicio de mantenimiento, reparando y/o reponiendo a costo propio todos los elementos dañados o ausentes.

El oferente deberá brindar al INSTITUTO, todos los informes que le sean solicitados.

La empresa vencedora de la presente licitación, tendrá a su exclusivo cargo el mantenimiento en forma íntegra, con materiales.

El INSTITUTO, a través de su personal (Departamento Seguridad de Juego) requerirá y fiscalizará las prestaciones de este servicio en las condiciones enunciadas en el presente.



### **Alcance**

La presente especificación tendrá alcance a las actividades de mantenimiento vinculadas al sistema de CCTV y sus accesorios, en los Casino alcanzados por la presente licitación.

### **Contratación**

La contratación se efectuará en la modalidad indicada en el anexo B.

### **Lugar de prestación del servicio.**

El mantenimiento preventivo se realizará en el o los lugares que designe el a una dirección de correo electrónico indicada por el INSTITUTO. Los mismos serán indicados en el anexo B.

### **Técnicos responsables del mantenimiento.**

El oferente debe asignar un técnico responsable y un suplente del mismo que respondan los requerimientos de mantenimiento correctivo generados por el Departamento Seguridad de Juego. El oferente debe indicar los números de teléfono tanto del responsable, como así también, el del suplente, brindando además, los canales alternativos de comunicación que existan para ubicarlos.

Es responsabilidad de oferente que los llamados sean atendidos por personal técnico capacitado para la labor que se requiere y que los mismos cumplan con los requerimientos del anexo C.

### **Consideraciones finales del mantenimiento.**

En caso de fallas insalvables en las cámaras analógicas, su reemplazo se realizará por cámaras con tecnología nueva y se irán incorporando progresivamente a los equipos NVR/servers.

Se realizarán informes técnicos internos, contestaciones de oficios judiciales, se deberá brindar respuesta a puntos de pericia y cuanto resulte necesario para



acreditar la validez de la prueba fílmica, conforme fuera solicitado por el área de legales.

Se deberá concurrir a reuniones, mediaciones y audiencias judiciales, con equipos de reproducción propios, a fin de asistir a las áreas legales o autoridades periciales, en la exposición de video filmaciones, explicando, la inviolabilidad del sistema y sus principales características técnicas.

Elaboración y presentación inmediata de cuanto material fílmico de archivo le sea solicitado por el Departamento Seguridad de Juego, incluyendo las tareas de compilación y cualquier otra que fuese necesaria para cumplimentar la solicitud.

#### **Informe de inicio de mantenimiento.**

Se requiere como primera medida, la confección de un informe que sea producto de un relevamiento minucioso y que documente el estado inicial de todos los elementos a los cuales se va a brindar el servicio de mantenimiento, indicando por cada uno de ellos, marca, modelo, número de serie y ubicación.

También se deben documentar los parámetros de configuración más importantes de cada uno de los equipos, rótulos, direcciones IP, Resolución, FPS, etc.

Adjunto al informe de inicio de mantenimiento se debe adjuntar un cronograma que indique el orden en el que se efectuará la recorrida de mantenimiento preventivo indicando las fechas en las que se visitará cada punto.

El informe debe ser entregado en el tiempo de presentación del informe de inicio de mantenimiento indicado en el anexo A.

#### **Mantenimiento preventivo**

Se requiere que el mantenimiento preventivo, sea efectuado con la frecuencia indicada en el anexo A. Entregando mensualmente planillas que documenten con fecha y hora, la recorrida de todos los elementos que componen el sistema de CCTV.



Estas planillas deben ser presentadas el primer día de cada mes, para certificar los trabajos realizados.

Se requiere planillas de mantenimiento preventivo de:

Cámaras.

Grabadoras de video.

Fuente de alimentación / Transformadores.

Las tareas que se deben llevar a cabo dentro del mantenimiento preventivo son:

Verificación y ajuste de fecha y hora del sistema.

Inspección ocular de los equipos que componen el sistema (Cámaras, Grabadoras, Fuentes de Alimentación, Transformadores, Estaciones de Monitoreo, Monitores, Joystick / Teclados, etc).

Inspección ocular de los elementos de sujeción (tornillos, soportes, etc)

Limpieza de todos los elementos que componen el sistema.

Limpieza de los recintos que alojan grabadoras o cualquier tipo de fuente de alimentación o Transformador correspondiente al sistema.

Verificación del video en vivo de todas las cámaras.

Verificación de orientación, zoom y foco de todas las cámaras.

Revisión de la cantidad de días / horas de grabación disponibles en cada grabadora.

Revisión del registro de actividad de la grabadora.

Medición de la tensión de salida de las fuentes de alimentación.

Verificación de gabinetes y cerraduras.

Confección de planillas que documenten las tareas de mantenimiento.



Generación de un parte diario de novedades sobre el sistema.

El corriente documento indica todos los ítems que el INSTITUTO, desea que el oferente controle y mantenga.

La verificación y ajuste de hora del sistema, debe realizarse utilizando una fuente de hora confiable. El oferente debe elegir una única fuente de hora para todas las verificaciones de horario que se realicen.

Inspección óptica de todos los elementos que componen el sistema para determinar su existencia y verificar si los mismos fueron o no dañados por factores climáticos, actos de vandalismo y/o cualquier otro factor que pudiera alterar el normal funcionamiento del bien.

Se requiere también la inspección ocular de todos los elementos de sujeción del sistema, tornillos abrazaderas, soportes y cualquier tipo de elemento de anclaje que se hayan utilizado. Si eventualmente se detectara que alguno de estos elementos no existe o no se encuentra en condiciones, debe ser reemplazado a costo del oferente.

Se debe eliminar todo tipo de suciedad, polvo, telarañas, pelusas o cualquier otro elemento extraño. La limpieza debe contemplar todos los elementos asociados a la cámara, Gabinete, Burbujas de protección, Soportes, Lentes, Fuente de alimentación / Transformadores.

Se debe mantener libre de todo tipo de suciedad, polvo, telarañas, pelusas o cualquier otro elemento extraño, los recintos donde se encuentran alojados las fuentes y las grabadoras de video.

La limpieza debe realizarse removiendo la suciedad y evitando que la misma se deposite sobre otros elementos.

Se debe revisar el video proveniente de cada una de las cámaras, para garantizar que las imágenes sean óptimas para ser grabadas. En este punto además del foco



de las lentes, se debe revisar el ángulo de cobertura de la cámara sea el correcto y que además se encuentre orientada de manera apropiada.

También debe verificar que la imagen proveniente de las cámaras no se encuentre alterada por interferencias de origen eléctrico.

Como parte de la rutina de mantenimiento preventivo, se debe verificar cual es la cantidad de días/horas que se encuentran almacenados en cada uno de los equipos de grabación de video.

También se debe revisar el registro de actividad de cada equipo, para determinar si el equipo presentó fallas durante el tiempo transcurrido desde la última revisión.

El oferente tiene también a su cargo el mantenimiento de todas las cerraduras y gabinetes que contengan cualquier dispositivo correspondiente al sistema de CCTV. Los gabinetes deben mantenerse en condiciones tales que permitan el resguardo de los equipos ante factores climáticos y/o vandalismo.

Los gabinetes de las cámaras deben también permitir la correcta visión de las mismas, quedando a cargo del oferente el pulido o reemplazo de vidrios y/o burbujas.

Se requiere la confección de planillas de mantenimiento preventivo para documentar la realización de todas las tareas de mantenimientos solicitadas, estas planillas deben estar aprobadas por personal designado por el INSTITUTO, todos los elementos que figuran en las planillas deben estar identificados tanto por su número de serie como también por su número de bien asignado por el departamento de patrimonio.

Se requiere también un parte de novedades correspondiente a cada jornada de mantenimiento.

Las tareas de mantenimiento no deben acarrear ningún tipo de costo para el INSTITUTO.



Todos los elementos necesarios para llevar a cabo esta labor corren por cuenta del oferente.

Además de las tareas de mantenimiento preventivo expresadas en este documento, el oferente tiene la libertad de agregar a la rutina de mantenimiento cualquier otra tarea que considere necesaria para preservar los bienes sobre los cuales presta servicio.

El oferente debe contar con todas las herramientas, equipamiento, software, medios de elevación, movilidad propia, equipos de comunicación o cualquier otro elemento necesario para brindar correctamente el servicio de mantenimiento.

Es responsabilidad del oferente mantener al día la documentación requerida por el Departamento de Seguridad e Higiene.

### **Mantenimiento correctivo**

El servicio de mantenimiento correctivo debe brindarse en la modalidad de mantenimiento con muletos (componentes de reemplazo transitorios), repuestos y/o reemplazo de equipamiento a cargo del oferente.

El INSTITUTO, se hará cargo solo de los equipos que sean sustraídos o dañados intencionalmente por terceros o por impericia de su personal. Para lo cual, será necesario un listado de equipos y materiales con costos asociados, para la pronta reposición de los mismos.

Los elementos que requieran mantenimiento correctivo, deben quedar operativos en el "Tiempo de ajuste, reparación o reemplazo por muleto", indicados en el anexo A.

Los equipos que se encuentren en falla, deben ser retirados para su reparación en el laboratorio del oferente, habiendo sido reemplazado previamente por un equipo muleto propiedad del oferente con las mismas características del equipo que se está retirando para su reparación, de forma tal que no se afecte a la operatoria. Los equipos muleto deben ser configurados de modo tal que el reemplazo sea



trasparente al usuario manteniendo todas las configuraciones idénticas al equipo retirado para su reparación.

Si el oferente determina que el equipo retirado es irreparable, debe reemplazar el mismo a su costo por uno de similares características.

Si el equipo en falla fuese un grabador de video, las unidades de almacenamiento que albergan las grabaciones, deben ser extraídas y entregadas al personal designado por el INSTITUTO, para ponerlas al resguardo. Si se determina que las unidades de almacenamiento son el causal de la falla del equipo, el oferente debe reemplazarlos a su costo quedando las unidades de almacenamiento dañadas en custodia del personal del Departamento de Seguridad de Juego.

La base de datos de imágenes de la grabadora muleto no debe ser borrada por ningún motivo, este debe resguardar las imágenes de los últimos veintiún (21) días.

La grabadora muleto debe ir acompañada de una planilla que documente con fecha y hora todos los lugares donde la misma fue instalada.

Cada vez que una grabadora muleto sea reubicada, se debe entregar una copia de la planilla vía e-mail a una dirección de correo electrónico indicada por el INSTITUTO. Se requiere también la confección y mantenimiento de una planilla que documente la ubicación actual de cada uno de los equipos muletos.

Cada vez que exista alguna modificación en esta planilla la misma debe ser enviada vía e-mail a una dirección de correo electrónica indicada por el INSTITUTO.

Cuando una grabadora de video pierda por cualquier causa las imágenes contenidas en sus unidades de almacenamiento, el prestador del servicio debe entregar dentro de las 24Hs un Informe que documente el causal de la ausencia de la información contenida dentro de la grabadora. Este informe técnico debe tener el membrete de la empresa que presta el servicio y debe ir firmado y sellado por el responsable de la misma.



El oferente debe atender los requerimientos de mantenimiento correctivo generados por el Departamento Seguridad de Juego, los mismos pueden ser realizado por:

Notificación escrita firmada con fecha y hora.

Vía e-mail a la dirección designada por el oferente.

Mediante llamada telefónica confirmada con fecha y hora de recepción.

Los requerimientos de mantenimiento correctivo, deben ser satisfechos en el “Tiempo de ajuste, reparación o reemplazo por muleto” indicado en el anexo A.

Anexo A

Tiempo de respuesta de mantenimiento.

Frecuencia de mantenimiento preventivo	1 mes.
Plazo de normalización total del servicio de CCTV	15 días.
Tiempo de extracción de video y entrega en formato físico	6 horas.
Tiempo de presentación del informe de inicio de mantenimiento.	7 días.
Tiempo de ajuste, reparación o reemplazo por muleto:	6 horas.
Reparación o reemplazo definitivo del bien con falla irreparable.	7 días.

Lapsos de prestación del servicio de mantenimiento.

El mantenimiento se debe prestar cumpliendo con la siguiente especificación de tiempo.

Día	Hora de inicio	Hora de finalización



Lunes	4:00	10:00
Martes	4:00	10:00
Miércoles	4:00	10:00
Jueves	4:00	10:00
Viernes	4:00	10:00
Sábado	4:00	10:00
Domingo	4:00	10:00
Feriado	4:00	10:00

#### Anexo B

Alcance del servicio de mantenimiento.

La presente contratación incluye todas las instalaciones estáticas de CCTV instaladas en los Casinos alcanzados por la presente licitación.

A modo general las mismas se efectuarán sobre:

- Cámaras e instalaciones en las Salas de Juegos.
- Cámaras e instalaciones en Cajas y Tesoros.
- Cámaras e instalaciones en Pasillos Interiores.
- Cámaras e instalaciones en Puertas de Ingreso/Egreso de Público,

Personal y/o proveedores.

- Cámaras e instalaciones en el exterior de los Casinos alcanzados.
- Sistema VMS



- Server para el Comand Center Site Server (Servicio del Centro de Comando).
- PC de clientes.
- DVRs/NVRs locales, sus instalaciones y elementos de protección
- Elementos anexos de instalación en los cielorrasos del Complejo Casino
- Monitores – Estaciones de Monitoreo – Estaciones de Edición y Salas de Rack's.

Los oferentes que hayan realizado la visita a obra, pueden solicitar una planilla electrónica complementaria con el detalle de cantidad de equipamiento que se debe mantener.

Lugar de prestación del servicio de mantenimiento.

El servicio de mantenimiento correctivo se debe efectuar en el lugar donde se encuentren los equipos, salvo aquellos que requieran ser trasladados al Laboratorio Técnico de la empresa proveedora.

Anexo C

Requerimientos complementarios.

El contratista deberá entregar una nómina en donde indique el título técnico de cada empleado afectado al mantenimiento, indicando sobre que sistema esta especializado.

Todo el personal del Contratista deberá estar contratado de acuerdo a las leyes vigentes.

Anexo D

Documentación a entregar conjuntamente con la oferta.



Tabla con las cantidades totales de todos los equipos a proveer indicando marca y modelo de los mismos.

Tabla con las cantidades totales de todos los equipos existentes a reutilizar indicando marca y modelo de los mismos.

Diagramas unifilares típicos en donde se documente como se van a conectar los equipos.

Diagrama de red de cámaras.

Carta del fabricante que acredite la inalterabilidad de la información de video contenida en el NVR y/o base de datos del VMS para que pueda ser utilizada como prueba ante la justicia.

Documentación a entregar al finalizar la obra.

Planos de ubicación en donde figuren los elementos provistos identificados por su número de serie.

Planos unifilares en donde se detalle la forma en la que se encuentran interconectados todos los elementos provistos.

Informe de medición del tendido de F.O. con OTDR en donde se pueda verificar la atenuación de cada pelo identificado también los lugares que son vinculados por los mismos.

Certificación de Cat6 del tendido de red de cobre.

Constancia de las capacitaciones.

Constancia de recepción de Manuales de Operación y Administración de los equipos.

Constancia de recepción de las licencias de software.

Planilla de cableado en donde se indique sobre que cable se encuentra conectada cada una de las cámaras.



## **ARTÍCULO 10°: INSTALACIÓN, FUNCIONAMIENTO Y MANTENIMIENTO DE SISTEMAS DE CONTROL DE ACCESO.**

La provisión, instalación, funcionamiento y mantenimiento integral de un Sistema de Control de Acceso Biométrico, para el registrar y controlar el presentismo, asistencia y permanencia, así como la fiscalización de seguridad relacionadas con el control de ingreso/egreso, con relación al personal del INSTITUTO, de la empresa, visitantes y proveedores en los accesos y áreas restringidas que se detallarán; puertas de ingreso/egreso de Personal; Tesoros; Cajas; y Áreas de Gerencia y oficinas, de todos los Casinos objeto de la presente licitación.

El mantenimiento estará a cargo del adjudicatario durante el período de garantía especificado en el presente artículo.

### **GENERALIDADES:**

La presentación de la propuesta implica que el adjudicatario estudió las especificaciones técnicas y realizó los relevamientos necesarios para evaluar el alcance de la contratación. El adjudicatario deberá ser representante oficial del fabricante de la solución ofertada, debiendo acreditar tal condición con la presentación de una carta de referencia del mismo, siendo dicha exigencia de carácter obligatoria. Asimismo, deberá poseer laboratorio homologado por los fabricantes para las tareas de mantenimiento y reparación.

El adjudicatario deberá también, como condición, presentar documentación que acredite haber efectuado al menos 5 (cinco) implementaciones de características similares a las de este requerimiento; sea ya ejecutadas o en proceso de implementación, solicitándose como preferencia mínimamente 2 (dos) de ellas sean en Casinos de dotaciones de personal similares. Deberán incluirse en cada antecedente contactos específicos a los fines de validar los mismos.

El adjudicatario es plenamente responsable de la idoneidad y suficiencia del equipo de trabajo, materiales, instalaciones y personal empleado.



Los trabajos deben ser completos y deberán considerarse incluidos todos los elementos y trabajos necesarios para el correcto funcionamiento, aun cuando no se mencionen explícitamente en pliego o planos.

#### ALCANCE DE LOS TRABAJOS:

- Provisión e instalación de unidades lectoras de IPB y EIP.
- Provisión e instalación de unidades controladoras.
- Provisión e instalación de barreras vehiculares.
- Provisión, instalación y puesta en marcha del conjunto de módulos de software.
- Integración con el sistema CCTV instalado.
- Instalación, cableado, etiquetado e interconexión de dispositivos.
- Adecuación de la red de suministro eléctrico y datos.
- Provisión e instalación del equipamiento de electrónica de red necesario para la interconexión del conjunto (control de acceso y CCTV) a la red de datos del INSTITUTO.
- Configuración de los equipos PC de escritorio destinados a los puestos de control y monitoreo del sistema de control de acceso.
- Capacitación de personal para operación y mantenimiento del sistema.
- Provisión e instalación de accesorios.

Todos aquellos accesorios, que, aunque no fueren mencionados en el corriente pliego, sean necesarios para el funcionamiento operacional del sistema.

- Programación, puesta en marcha y pruebas del sistema.
- Mantenimiento del sistema.



### PLANOS:

El adjudicatario, al recepcionar la Orden de Compra, deberá entregar al INSTITUTO para su aprobación, los planos de las instalaciones en formato digital y una copia, escala 1:200 para los planos de planta y 1:10 para los planos de detalle.

Todas las instalaciones deberán ser debidamente acotadas, ejecutándose también los planos de detalles necesarios o requeridos.

Antes de ejecutar sus planos, y antes de efectuar la compra de materiales, el adjudicatario deberá replantear en el lugar de los trabajos la totalidad de medidas físicas y eléctricas.

El INSTITUTO tendrá diez (10) días para proceder a la aprobación o rechazo de los planos.

La aprobación de los planos por parte del INSTITUTO no exime al adjudicatario de su responsabilidad por el fiel cumplimiento del pliego y planos y su obligación de coordinar sus trabajos con los demás gremios, evitando los conflictos o trabajos superpuestos o incompletos.

Los planos así presentados podrán recibir las siguientes calificaciones de parte del INSTITUTO:

Aprobado: sirve para iniciar la obra.

Aprobado con observaciones: puede comenzar los trabajos con los siguientes requerimientos

Debe presentar el plano corregido dentro de los 5 días corridos siguientes.

Deben tenerse en cuenta las observaciones realizadas, tanto en plano como en el lugar de trabajo.

Observado: no pueden comenzar la ejecución de los trabajos y debe presentarse urgente revisión, atendiendo a las observaciones. No da lugar a prórroga de plazos.



Durante el transcurso de los trabajos, se mantendrán al día los planos de acuerdo a las modificaciones necesarias y ordenadas.

Una vez terminadas las instalaciones, el adjudicatario entregará al INSTITUTO tres juegos ploteados de planos de las instalaciones estrictamente conforme a los trabajos realizados, más dos juegos de planos almacenados en archivo óptico, con todos los planos en cada juego, todo en Autocad 2010 o compatible.

#### NORMAS PARA MATERIALES Y EJECUCIÓN DE LOS TRABAJOS:

Los equipos estarán homologados según lo estipulado por estándares de calidad reconocidos.

Todos los trabajos serán ejecutados de acuerdo a las reglas del buen arte y presentarán, una vez terminados, un aspecto prolijo y mecánicamente resistente.

Los materiales y elementos ofertados deberán ser nuevos, completos, sin uso, estar en perfecto estado de funcionamiento y conforme a las normas indicadas en el ítem correspondiente o de aplicación.

#### MATERIALES:

En su propuesta el adjudicatario indicará las marcas de la totalidad de los materiales que propone instalar, y la aceptación de la propuesta sin observaciones no exime al Oferente de su responsabilidad por la calidad y características técnicas establecidas y/o implícitas en pliego y planos.

La totalidad de los materiales ofertados deben estar en producción al momento de la instalación, no se aceptarán, bajo ningún concepto, materiales cuya producción se encuentre discontinuada o próxima a su discontinuación.

Las características que se detallan, son de carácter general, debiendo el Oferente adjuntar a su propuesta planilla de características técnicas de los distintos elementos en calidad de datos garantizados, pudiendo el INSTITUTO pedir el ensayo de cualquier dispositivo y rechazar todo aquello que no cumpla los datos garantizados.



En los casos en que este pliego o en los planos se citan modelos o marcas comerciales, es al solo efecto de fijar normas de construcción o tipos de formas deseadas, pero no implica el compromiso de aceptar tales materiales si no cumplen con las normas de calidad o características requeridas.

Todos los materiales desmontados, y que no esté prevista en este pliego su reutilización, deberán ser entregados en el lugar a designar por el comitente (dentro del predio del Casino), limpios, acondicionados e inventariados.

El INSTITUTO se reserva el derecho de solicitar muestras de dichos materiales, si lo considera necesario para su aprobación.

#### MANUALES DE MANTENIMIENTO Y OPERACIÓN:

El Adjudicatario entregará para el software y para cada equipo electromecánico, o electrónico, antes de los ensayos de la instalación, un manual de operación y mantenimiento y la descripción del equipo en idioma castellano. Se entregará un digital y dos copias.

Dicho manual brindará, como mínimo, la siguiente información:

Instrucciones para el reemplazo de cualquier componente del sistema, incluso piezas internas.

Instrucciones para la limpieza y el ajuste periódico del equipamiento, bajo su respectivo cronograma.

Lista completa de todos los equipos y componentes, informando los domicilios y teléfonos de los fabricantes y proveedores respectivos.

Instrucciones operativas para el usuario, las cuales deben ser accesibles, cercanas a los puntos de operación.

#### INSPECCIONES:



Además de las inspecciones que a su exclusivo juicio disponga realizar el INSTITUTO, el Adjudicatario deberá solicitar con la debida anticipación, las siguientes inspecciones:

A la llegada de las distintas partidas de materiales para su contraste con respecto a las muestras aprobadas.

Al terminar el montaje de cada puesto de control, y luego de este, antes de poner en servicio.

Cuando hayan terminado la totalidad de los trabajos.

#### DESCRIPCIÓN DEL SISTEMA:

El sistema deberá tener capacidad de habilitar, registrar y procesar la información referida al ingreso, permanencia y egreso de personas en el edificio y las áreas restringidas dentro del mismo, así como el monitoreo de alarmas propias del sistema de Control de Acceso y gestión integral de seguridad y vigilancia, integrándose a su vez al sistema CCTV para lograr una solución adecuada.

Deberá funcionar como un sistema integrado, permitiendo que las personas, con la identificación personal biométrica autorizada (en adelante IPB, basado en una o más huellas dactilares de cada agente) y/o el elemento de identificación personal autorizado (en adelante EIP, basado en una credencial de proximidad) puedan ingresar en cualquiera de los accesos habilitados a tal fin. En el caso de existir distintos edificios, éstos deberán comunicarse utilizando los vínculos de la red de datos del establecimiento. La restricción de ingreso y egreso dependiendo la entrada (empleados, visitas) deberá ser configurable según requerimientos del organismo y poder realizarse desde el software.

Los eventos, ingreso y egreso, alarmas del sistema e imágenes del CCTV, etc., serán registrados automáticamente en cada uno de los puntos de acceso (área controlada con uno o más lectores) al edificio o áreas restringidas, para lo cual deberá coordinarse con las áreas respectivas vinculadas a Sistemas para asegurar vínculos controlados tanto a nivel de tráfico como de seguridad informática.



Debiendo el adjudicatario garantizar la seguridad requerida en la solución propuesta, hasta la conexión proporcionada por el INSTITUTO. Además, ambos sistemas, control de acceso y CCTV, deberán contar con sincronización horaria, la cual permita una concordancia horaria entre los eventos originados por el sistema de control de accesos y las imágenes capturadas por el sistema CCTV. Dicha sincronización horaria deberá implementarse de manera nativa o mediante configuración externa.

El sistema deberá minimizar las molestias y demoras a los peatones sin perder por ello cantidad de información obtenida y confiabilidad respecto de la seguridad.

La identificación del personal se realizará exclusivamente a través de la Identificación Personal Biométrica (IPB, basado en una o más huellas dactilares de cada agente). No obstante, para el caso de un agente que por cuestiones físicas (temporales o permanentes), no pueda utilizar su huella dactilar para ser enrolado o para acceder en determinado momento, se utilizará como Elemento de Identificación Personal (EIP) una credencial de proximidad.

Para las visitas y contratistas deberán utilizarse tarjetas como único EIP, que lo devolverán al retirarse y al finalizar sus tareas en el edificio, a través de un buzón de visitas en los molinetes.

El sistema deberá permitir determinar en todo momento qué personas se encuentran dentro del edificio y/o áreas restringidas, a través de la emisión de informes basados en los últimos estados registrados de circulación o marcación

El re arranque del sistema, luego de un corte de energía, deberá ser similar al arranque normal del sistema, no debiéndose requerir procedimientos especiales como reconstrucción, recuperación o reorganización de archivos. Todas las cerraduras eléctricas quedarán abiertas en caso de falta de energía, y deberán asegurarse los medios adecuados para la apertura en dirección salida en caso de emergencias.



El sistema deberá ser integralmente compatible con el sistema de control de acceso biométrico implementado en el INSTITUTO en su sede de La Plata cita en calle 46 n° 581, y asimismo, deberá garantizarse la interoperabilidad con sistemas existentes y otros a implementarse.

Asimismo, el sistema de control de acceso ofrecido deberá:

- Incluir todos los Kit de Desarrollo de Software (SDK) necesarios para desarrollos de aplicativos de software basados en DLLs, controles ActiveX u otra solución que pueda integrarse fácilmente a entornos de desarrollo.NET, Java, etc.
- Permitir liberar todas las barreras, molinetes y puertas que se encuentren alcanzadas por el mismo ante situaciones de emergencia, desde el software de gestión.
- Permitir un método de control de asistencia y permanencia del personal efectivo y práctico en su operatividad.
- Brindar una función de seguridad indispensable para el control de personal que circula por áreas con manejo de valores y/o de accesos restringidos
- Utilizar paneles de control de acceso que se mantengan operativos aun cuando el servidor se encuentre fuera de línea.
- Contar con un software de gestión que provea soporte para configuración en múltiples tipos de Base de Datos: SQL Server, Oracle, etc.
- Tener la capacidad de control de ascensores, pudiendo interactuar con la CPU del ascensor para que el teclado del ascensor habilite solo para los pisos en los que la Identificación Personal Biométrica (en adelante IPB, basado en una o más huellas dactilares de cada agente) y/o el Elemento de Identificación Personal (en adelante EIP, basado en una credencial de proximidad) esté autorizado y reporte al sistema el piso elegido en forma instantánea.



- Poseer software cliente que permita ver las fotos de las personas en el momento en el que estas presentan su IPB y/o EIP en alguna lectora.
- Permitir un mínimo de 20 clientes simultáneos del sistema (con posibilidad de ampliación)
- Permitir configurar la búsqueda en la base de datos o concentradores hasta en un % de coincidencia.
- Cumplir con las especificaciones técnicas y de funcionalidad que se piden en este pliego

## **DESCRIPCIÓN Y FUNCIONALIDAD DE PUESTOS**

### **PUESTO LOCAL DE CONTROL:**

Es el lugar físico donde se realiza la gestión y monitoreo del punto de acceso bajo su jurisdicción y en él se instalará todo el equipamiento y software necesario para cumplir con la totalidad de las funciones requeridas.

### **FUNCIONES:**

Monitorear la totalidad de la información que se genera por el ingreso o egreso de personas, registro de los materiales y/o elementos ingresados por un visitante, eventos de alarma propios del sistema de Control de Accesos, e imágenes del CCTV correspondientes al punto de acceso bajo su jurisdicción.

Ingresar al sistema la información relativa a las visitas según el procedimiento indicado en el presente pliego.

Ingresar al sistema la información relativa a materiales y/o pertenencias según el procedimiento indicado en el presente pliego.

Ingresar al sistema la información relativa al personal para los casos de tratamiento especial y según el procedimiento indicado en el presente pliego.



Realizar acceso manual a empleados, con la finalidad de solucionar problemas de antipassback.

#### ELEMENTOS COMPONENTES:

Se instalarán e integrarán todos los elementos componentes necesarios para cumplir con las funciones indicadas, además de los que se describen a continuación.

Mostrador y delimitadores de acceso.

Se utilizarán los existentes para la operación y atención de usuarios y visitas.

Equipamiento para captura de imágenes.

A los efectos de capturar una imagen digital de pertenencias, suministros y visitas, se utilizarán las cámaras a proveer.

Equipamiento para el ingreso automático de las tarjetas RFID para visitantes, a través de un emulador de teclado.

A los efectos de capturar el número y asignación de credenciales a visitantes se utilizarán los lectores de conexión USB descriptos.

Dispositivos ante emergencia.

Se integrará al sistema un pulsador del tipo "golpe de puño", el cual permitirá habilitar todas las salidas controladas por el puesto, ante una emergencia.

#### PUESTO CENTRAL DE CONTROL.

Es el lugar físico donde se realiza la gestión y administración necesaria para cumplir con todas las funciones requeridas en este puesto, además de poder realizar todas las funciones de un puesto local en forma remota.

#### FUNCIONES:



Gestión y configuración integral de la totalidad del sistema de control de acceso.

Almacenar, procesar y monitorear la totalidad de la información que se genera por el ingreso o egreso de personas, por eventos de alarma y demás información generada por cualquiera de las partes componentes del sistema.

Almacenar y actualizar la información correspondiente a las personas, ya sea en forma permanente o transitoria, así como su categoría frente al sistema de control de acceso.

Realizar el control centralizado de todos los dispositivos para la conformación de barreras físicas de acceso al edificio y áreas restringidas.

Generación de reportes

Enrolamiento del personal.

Entrega de credenciales.

Establecer la comunicación simétrica y asimétrica, a través de la red de datos propia del Organismo a los efectos de brindar acceso a las bases de datos generadas por el sistema desde otras aplicaciones.

#### ELEMENTOS COMPONENTES:

Se instalarán e integrarán todos los elementos componentes necesarios para cumplir con las funciones indicadas, además de los que se describen a continuación.

- Mostrador y delimitadores de acceso.

Se utilizarán los existentes para la operación y atención de usuarios y visitas.

- Equipamiento para captura de imágenes.

A los efectos de capturar una imagen digital de pertenencias, suministros y visitas, se utilizarán las cámaras a proveer.



- Equipamiento para el ingreso automático de las tarjetas RFID para visitantes, a través de un emulador de teclado.

A los efectos de capturar el número y asignación de credenciales a visitantes se utilizarán los lectores de conexión USB descriptos.

- Dispositivos ante emergencia.

Se integrará al sistema un pulsador del tipo “golpe de puño”, el cual permitirá habilitar todas las salidas controladas por el puesto, ante una emergencia.

#### PROVISIÓN, INSTALACIÓN Y FUNCIONAMIENTO DEL CONJUNTO DE MÓDULOS DE SOFTWARE

Se incluye la provisión, instalación y puesta en marcha de la totalidad del software de aplicaciones y bases de datos para cumplir con la totalidad de las funciones requeridas.

#### PRESTACIONES GENERALES:

El sistema debe ser web y deberá tener la posibilidad de funcionar sobre servidores virtualizados. Se debe prever la posibilidad de aumentar la capacidad instalada en por lo menos un 50% sin necesidad de modificación del software o hardware y sin perder performance.

El software correrá sobre SISTEMAS OPERATIVOS ENTORNO Windows/LINUX.

El Oferente deberá garantizar la seguridad de la información y operación desde sus interfaces, generando bitácoras que detallen qué operadores efectuaron qué operaciones principales, con un nivel de detalle suficiente que permita una adecuada auditoría, incluyendo información sobre quien, en donde y en qué momento se modificó información en el sistema, permitiendo reportes de esta información.



Todos los módulos de control de accesos, visitantes y asistencia, estarán integrados entre sí. Y podrán relacionarse con otros sistemas, a nivel bases de datos, utilizando las API o interfaces adecuadas.

El Oferente deberá indicar en su oferta el hardware de servidores que es necesario para soportar el software cotizado, garantizando el desempeño solicitado del sistema.

Se deberá garantizar la compatibilidad del software con el hardware ofertado en un 100 %.

#### CARACTERÍSTICAS Y MÓDULOS DEL SISTEMA:

- Licencia: gratuita.
- Base de Datos: MSSQL, MySQL y Oracle
- Máximo de Dispositivos: 512
- Clientes Concurrentes: ilimitado
- Seguridad integrada por LDAP
- El software deberá contemplar como mínimo los siguientes módulos y aplicaciones:
  - Administración de Usuarios
    1. Soporte N niveles de departamentos
    2. Interfaz de búsqueda de usuario
    3. Configuraciones de administrador multi-nivel
    4. Modo de autenticación personalizada por el usuario
- Gestión del Control de Acceso
  1. Controla hasta 128 grupos de acceso



2. Controla hasta 128 calendarios
  3. Configurar Días festivos.
- Enrolamiento y credencialización de personal.
  - Gestión de visitas.
  - Administración de Puertas
    1. Grupos de hasta 4 niveles de puerta
    2. Controla hasta 512 puertas
    3. Funcionalidad de configuración de alarma para puertas seleccionadas
  - Administración de ascensores.
  - Administración de dispositivos.
    1. Configuraciones de dispositivos de control de acceso e I/O
    2. Soporte RS485 hasta para 8 dispositivos
    3. Monitoreo en tiempo real de conexión de dispositivos
    4. Interfaz de búsqueda de dispositivo de tipo asistente
    5. Fácil actualización de firmware y reinicio
  - Interfaz de Mapa Visual - Presentación gráfica del sistema:
    1. Cambio de configuración del dispositivo/puerta desde el mapa
    2. Monitoreo en el mapa, en tiempo real
    3. Notificaciones de eventos por medio de íconos gráficos



4. Interfaz de monitoreo para puertas y zonas
  5. Integración con Cámaras IP y NVR (Grabador de Video en Red)
  6. Monitoreo de video en tiempo real
  7. Captura de imagen estática en eventos predeterminados
  8. Soporta configuración de eventos con terminales de acceso nominadas
- Integración con otros proveedores.
  - Monitoreo de Eventos y Alarmas, relacionadas al Control de Accesos.
  - Generación de reportes de tiempos y asistencias.
    1. Interfaces con sistema de ABM CENTRAL -Tiempo y Asistencia – Novedades (ver Anexo I: REQUERIMIENTOS DE INTERFASE SIAPE- SISTEMA DE CONTROL DE ACCESO).
  - Módulo de Reportes

#### **Servidor de control de accesos.**

**Tipo:** Rackeable

**Marca:** Primera marca (no se aceptará un clon)

#### **Detalle:**

- Procesador: Intel XeonQuad Core Processor E5504 (2.00 GHz, 4MB L3 Cache, 80W, DDR3-800) Memoria: 2 x 2GB PC3-10600E. Máxima: 144GB
- Disco rígido: 2 de 1,5 TB
- Controladora de disco: P410 Smart Array SAS/SATA RAID 0, 1, 10,5

137



- Interfaz de red: NC362i Integrated Dual Port Gigabit Server Adapter /
- Unidad óptica: DVD R/W
- Gabinete: Rack.1U

#### CAPACIDAD DEL SISTEMA:

El sistema central debe ser capaz de procesar como mínimo una cantidad de transacciones diarias, igual a 10 (diez) veces la suma de empleados y visitas.

El sistema debe contemplar, como mínimo, un volumen del 80% del personal que debe poder ingresar y/o egresar en un lapso máximo de 30 minutos.

Se debe prever la posibilidad de aumentar la capacidad instalada en por lo menos un 50%, sin necesidad de sustitución o modificación del software y cumpliendo con la totalidad de los requerimientos del presente pliego.

#### GESTIÓN DE CONTROL DE ACCESO:

Este software será el encargado de la gestión integral del sistema. Manejará todas las opciones de configuración y control de la totalidad de los dispositivos, de las bases de datos, e interfaces con otros sistemas. Permitirá la exportación de datos en formatos estándar (.csv, .txt, .xls, etc.).

#### GENERACIÓN DE LAS BASES DE DATOS:

Generación de Bases de Datos del personal, ingresando manualmente los campos propios del sistema e incorporación automática de los campos provenientes de bases de datos de otros sistemas en uso por el organismo, para lo cual deberá utilizar algún método ajustado de intercambio de información a nivel base de datos

Los campos provenientes de otros sistemas se actualizarán de forma automática, pre programada, así como cada vez que el operador lo disponga.

#### COMUNICACIÓN CON LOS CONTROLADORES:

138



El servidor podrá operar on-line con los controladores y/o comunicarse con cualquiera de ellos para la transmisión en batch de los registros almacenados en la memoria de los controladores. La comunicación batch podrá ser establecida en forma manual por el operador o activarse automáticamente en función del porcentaje de llenado del buffer del controlador o en horarios preestablecidos. La consulta on-line de los controladores no debe interrumpir la recepción de información desde los puestos de captura y/o monitoreo.

El modo principal de operación será on-line donde el servidor se comunicará en tiempo real toda la información necesaria para la autorización del ingreso/egreso de empleados y visitas.

#### PERMISOS DE ACCESO:

Los permisos de acceso, configurables por los usuarios se podrán establecer de manera general, grupal e incluso individual, pudiéndose otorgar los permisos de manera simplificada, por medio de operaciones drag & drop.

El sistema de control de accesos deberá permitir asignar fácilmente y a través del software permisos de acceso a los usuarios a una o un grupo de puertas durante:

- Una franja horaria.
- Uno o más días de la semana en particular.
- Una fecha o rango de fechas.
- Los feriados o días no laborables.
- Distintas combinaciones de los anteriores.

De forma tal que el personal no pueda acceder a lugares a los que no está autorizado o ingresar a través de puertas en las que usualmente tiene permiso en horarios en los que no está autorizado a ingresar.

#### ALTAS Y BAJAS DE ELEMENTOS DE IDENTIFICACIÓN PERSONAL (EIP) y DE IDENTIFICACIÓN PERSONAL BIOMÉTRICA (IPB):



Deberá registrarse cuando un EIP y/o IPB sea dado de alta y/o baja, y asociados entre sí. En el caso de baja se indicará el motivo de la misma, con opciones preestablecidas. Por ej. anulado, caducidad del contrato u otros. Deberá poder establecerse un período de vinculación entre un EIP y un determinado empleado.

El sistema de enrolamiento biométrico debe ser compatible en un 100% con la solución de control de accesos.

#### DETECCIÓN DE FALLA EN LOS FICHAJES:

El sistema poseerá la capacidad de análisis de los fichajes de los empleados, de manera tal de detectar inconsistencias en los movimientos de los empleados (entradas sin salida, salidas sin entrada, doble entrada, doble salida, entre otros).

#### MONITOREO DE EVENTOS Y ALARMAS:

Toda situación de alarma o evento que implique una situación excepcional a ser manejada por el operador, deberá registrarse y generar un aviso suficiente para su administración, y el sistema deberá permitir que diferentes usuarios observen una parcialidad o totalidad de estos eventos, en función de su nivel de responsabilidad o campo de control.

#### CONFIGURACIÓN DE ALARMAS:

Permitirá configurar en forma totalmente flexible, cuáles de los dispositivos de alarma serán activados en función de los siguientes datos: fecha, hora, punto de acceso, presencia o ausencia de operador local en el lugar de ocurrencia del evento y tipo de evento de alarma. La configuración del sistema de alarmas permitirá a su vez activar las salidas de contactos secos del sistema.

La activación de los dispositivos de alarma puede ser automática o requerir la intervención del operador, esto deberá ser configurable por software.

Podrán configurarse cuáles serán las instrucciones a seguir por el operador, luego de que el sistema identifique un evento de alarma, a fin de que el personal de operación tome acción según dichas instrucciones.



### ALARMAS:

Se podrán monitorear y registrar los siguientes eventos de alarma.

### EN LOS DISPOSITIVOS DE ACCESO PARA PERSONAS:

Intento de pasaje sin previa habilitación.

Intento de ingreso fuera del horario permitido.

Pasaje en el sentido opuesto al de la habilitación.

Presentación de IPB/EIP en un punto de acceso para el cual no está habilitado.

Intento de egreso sin haber registrado un ingreso (control antipassback).

Intento de ingreso sin haber registrado un egreso.

Presentación del IPB/EIP sin concretar el paso a través del acceso en un período de tiempo predeterminado y ajustable.

### EN LAS UNIDADES CONTROLADORAS:

Salida de operación de las líneas de comunicación y dispositivos que dependen de cada controlador.

Caída del puesto central de control o del enlace con el mismo.

Falla en el suministro de energía eléctrica. Deberá existir una alarma un tiempo programable antes del agotamiento de la batería.

Intento de desarme o rotura del controlador.

### ACCESO MANUAL:

En caso de configurarse al sistema para Control Antipassback en determinados perímetros controlados, se deberán proveer las herramientas informáticas necesarias para que los operadores habilitados puedan solucionar los inconvenientes derivados de una falta de marcación de Antipassback



### SOFTWARE DE VISITAS:

El sistema tendrá capacidad para llevar un registro de la totalidad de las visitas que ingresen al edificio y almacenar los datos.

Los datos a tomar en los puestos locales de control serán, como mínimo, los siguientes: apellido, nombre, DNI, foto, oficina y persona a visitar, motivo de la visita (seleccionable entre las opciones almacenadas), empresa, organización u organismo al que pertenece (seleccionables entre las opciones almacenadas), observaciones (mínimo 255 caracteres).

Permitirá:

Generar permisos adecuados sobre las puertas, barreras y/o molinetes que sean necesarios para que el visitante pueda moverse dentro del circuito de visita para el que se encuentra habilitado dentro de los horarios permitidos por dicho permiso.

Autorizar la salida del visitante en el momento en que este deposite la tarjeta de visita en el buzón colocado para tal fin, y al mismo tiempo deshabilitar la tarjeta para evitar que alguien pueda generar registros asociados al visitante cuando el mismo ya no se encuentre en el edificio.

Saber si la visita estuvo anteriormente en el edificio y en caso afirmativo presentar en el formulario los datos personales de la visita que se cargaron inicialmente.

Saber si la persona a visitar se encuentra en el edificio.

Comandar los dispositivos de captura de imágenes.

Contemplar un tratamiento diferencial para las personas que realicen trabajos temporarios dentro del edificio (contratistas). Este podrá ser un módulo independiente, o bien estar considerado dentro del módulo de visitas.

### GENERACIÓN DE REPORTE:



Independientemente de la aplicación que utilice el sistema deberá generar reportes desde plantillas pre cargadas propias de la solución y contar con la posibilidad de generar nuevas ad doc.

La información a consultar será en tiempo real.

La generación y visualización de reportes no debe interrumpir la actividad normal del sistema, y deben poder ser emitidos a demanda.

Todos los reportes podrán obtenerse por pantalla, impresora, medios de almacenamiento óptico o magnético, o ser transmitidos vía red (LAN) o por correo electrónico. Los archivos serán de formato estándar documentado, preferentemente .xml, .xls, .txt, .pdf, etc. para ser utilizados en ambientes multiplataforma.

#### BASES DE DATOS:

Deberán ser bidireccionales y asegurar la integridad referencial.

El Oferente presentará la estructura detallada de las bases de datos utilizadas, detallando campos, relaciones entre las distintas tablas y bases, claves principales, etc. Además, se entregarán las APIs o interfaces provistas y utilizadas para la conexión de las bases de datos. Las mismas deberán ser aprobadas por el comitente antes de su implementación.

#### ENROLAMIENTO BIOMÉTRICO DE PERSONAL:

Deberá evaluar e indicar la calidad de la huella enrolada y asociarla con todos los parámetros del empleado.

El sistema de enrolamiento biométrico debe ser compatible en un 100% con la solución de control de accesos.

La empresa Oferente deberá proveer los medios necesarios para garantizar la integridad y confidencialidad de la información de las huellas enroladas en el sistema.



El oferente deberá realizar el enrolamiento de al menos el 70% del personal actual del organismo. Realizando, a su vez, la capacitación adecuada del personal que se ocupe del relevamiento restante.

#### SOFTWARE DE ASISTENCIA:

El sistema tendrá capacidad para administrar el presentismo/ ausentismo del personal, pudiendo manejar una variedad de horarios, tipos de hora, justificativos de ausentismo, etc.

Deberá cumplir con los siguientes puntos:

Deberá tener una interfaz gráfica intuitiva, que permita las operaciones principales tanto en formato gráfico como textual.

Deberá admitir operaciones a nivel grupal o individual.

Se registrará el horario de entrada y salida de cada empleado y visita, cada vez que ingrese al edificio, indicando por cual entrada ingresó.

Para el caso del personal propio del organismo, deberá registrar el horario de ingreso/egreso indicando al menos TIPO INGRESO/EGRESO, FECHA DEL INGRESO/EGRESO, HORA DEL INGRESO/EGRESO, PUERTA O PUNTO DE ACCESO POR EL QUE SE REALIZO DICHO INGRESO/EGRESO.

Para el caso de la visita, deberá registrar el horario de ingreso/egreso indicando al menos TIPO INGRESO/EGRESO, FECHA DEL INGRESO/EGRESO, HORA DEL INGRESO/EGRESO, PUERTA O PUNTO DE ACCESO POR EL QUE SE REALIZO DICHO INGRESO/EGRESO.

Para el caso del personal propio del organismo, No se deberán implementar controles y/o restricciones sobre la FRANJA HORARIA de cumplimiento, ni limitaciones al respecto.

Tendrá funciones de seguridad para limitar el acceso por usuario a diferentes funciones del sistema y/o registros de personal.



Tendrá una herramienta de búsqueda rápida, sin emisión de informes en pantalla o papel, de anomalías, como marcaciones incompletas, llegadas tarde, ausentes sin justificar, etc.

Podrá generar informes de distinto tipo, exportables en diferentes formatos (.txt, .csv, .pdf, .xls, .doc, etc.).

Dispondrá de informes de índole estadístico, que permita observar la información de manera gráfica (a través de gráficos de barra, torta, o similares).

Los informes podrán filtrarse por diferentes categorías o áreas, pudiéndose luego generar un informe pre filtrado para su uso habitual.

Podrá agruparse a los registros de personal según la estructura jerárquica propia del organismo, en áreas y subáreas, formando un árbol jerárquico, que luego permita operaciones grupales, y emisión de informes con filtros.

El sistema deberá poder integrarse con el sistema de RRHH del organismo, tanto para obtener los registros de personal, como para exportar la información necesaria de las horas/días trabajados y su tipo, ausentes y sus causas, licencias, etc., para el sistema de liquidación de haberes.

El software ofrecido por la empresa, debe ser capaz de exportar los datos en distintos formatos (.txt, .xml, .xls) y dichos archivos exportados deberán tener la posibilidad de ser transferidos al Sistema Provincial de RRHH de la Provincia de Buenos Aires dependiente de la Dirección Provincial de Tecnologías y Operaciones de la Subsecretaría de Capital Humano del Ministerio de Economía. Teniendo en cuenta un periodo de prueba sobre dicha transferencia. Los métodos de transferencias están descriptos en el Anexo I.

#### DESARROLLO DE LAS TAREAS:

Los trabajos se desarrollarán por puesto de control. Las tareas necesarias para la implementación del nuevo sistema no deberán interferir con el funcionamiento del sistema actualmente instalado y deberán ser coordinadas con el INSTITUTO.



### ELEMENTOS DE IDENTIFICACIÓN PERSONAL (EIP)

Se utilizarán elementos de identificación personal (EIP) que poseerán únicamente los empleados que por cuestiones físicas (temporales o permanentes), no puedan utilizar su huella dactilar para ser enrolados o para acceder en determinado momento.

Dichos elementos son credenciales para lectura por RF de proximidad pasiva con tecnología Mifare /Iclass HID o IClass HID o equivalentes.

Se utilizarán elementos de identificación personal (EIP) que se les entregarán temporalmente a los visitantes al momento del ingreso y que poseerán durante su permanencia, los mismos serán introducidos en un buzón validador al momento del egreso, con el fin de su recuperación y reutilización. El sistema de control de visitas deberá dar automáticamente la baja del visitante al registrar el depósito de la credencial temporalmente asignada en el buzón.

Dichos elementos son credenciales para lectura por RF de proximidad pasiva con tecnología Mifare /Iclass HID o IClass HID o equivalentes.

Cada credencial de proximidad se identifica con un número único pregrabado por el fabricante, el que se informará al Oferente una vez se realice la carga masiva de información al nuevo sistema.

La codificación del número que identifica a cada credencial tiene como mínimo 37 dígitos binarios, y asegurar la no duplicidad de las credenciales. Ante la pérdida o rotura de una credencial, su reemplazo deberá tener un número diferente.

### PROVISIÓN E INSTALACIÓN DE UNIDADES LECTORAS DE EIP/IPB

Se deberán proveer e instalar unidades lectoras de EIP e IPB.

Serán del tipo de proximidad, salvo en aquellos casos en que se indique la utilización de otro tipo de tecnología.



Deben permitir, a partir de la lectura de un EIP, el envío de los datos de identificación de dicha EIP a las unidades controladoras, utilizando el protocolo de comunicación Wiegand.

Tiempo de lectura promedio inferior a 2 segundos.

Error de lectura inferior a 1%.

Ser aptas para montaje en exterior. Libre de mantenimiento en condiciones de trabajo y ambientales normales del organismo.

#### **LECTORES DE PROXIMIDAD:**

Para punto de control. (Molinetes, Puertas)

Lector de tecnología de 13.56 MHz, para lectura de tarjetas iCLASS y Mifare, o equivalentes.

Rango de lectura: mínimo 3, máximo 10 cm.

Salida: Wiegand.

Para Puesto de Enrolamiento (ENROL. TARJETAS USB).

Lector de tecnología de 13.56 MHz, para lectura de tarjetas iCLASS y Mifare, o equivalentes.

Rango de lectura: mínimo 3, máximo 10 cm.

Salida: USB 2.0

#### **LECTORES IPB - HUELLA DACTILAR:**



Se empleará como IPB del personal, MÍNIMO al menos dos de sus huellas dactilares (a determinar), las cuales serán expuestas al Lector para habilitación del acceso

Para punto de control. (Molinetes, Puertas)

Para registrar el acceso deberá proveerse el dispositivo con pantalla de más de una línea con la información básica para una marcación: fecha y hora del registro, y nombre y apellido de la persona reconocida.

Características:

Tipo de escáner Unidactilar.

Escáner de tecnología óptica de huella tipo touch, no susceptible a descargas electrostáticas (ESD)

Feedback: Debe contar con un indicador lumínico que indique la detección o falla de detección de la huella. Asimismo, deberá proveerse con pantalla de más de 1 línea. Además, el dispositivo deberá realizar indicaciones auditivas de los diferentes estados.

Deberá contar como mínimo con doble factor de autenticación, permitiendo utilizar alternativamente a la lectura de huella el ingreso de una lectura de credencial RFID. El mismo deberá poder ser configurado de manera particular por cada persona a autenticar

Tipo de Detección (1:1, 1:N), lectura de credencial RFID

Los templates almacenados no deberán incluir imágenes reales de la huella dactilar, sino únicamente los rasgos unívocos (minucias). Cada template, deberá contener al menos 350 bytes de información por cada huella.

En los dispositivos donde no llegue a consumir el 50% de la capacidad de templates, se deberá poder activar el modo adaptativo, ante el cual se almacenen localmente las huellas mejores al template almacenado en cada caso.



El enrolamiento se deberá poder realizar en cualquier dispositivo para control de asistencia, y los templates deberán quedar replicados tanto en el dispositivo, como en la base de datos, de modo de asegurar su resguardo y replicación en caso de ser necesario.

Almacenamiento en modo off line mínimo cincuenta mil (50.000) fichajes.

Capacidad de almacenaje propio: mínimo 4.500 USUARIOS a dos huellas por persona (9.000) huellas.

Tiempo de respuesta comprobable: menor o igual a dos (2) segundos en situación de saturación de la capacidad de almacenamiento.

Todos los dispositivos para marcación deberán poder operar autónomamente ante cortes de vínculo con el servidor central. Los que se utilicen para asistencia, deberán además poseer backup energético propio asegurando una autonomía mínima de 2 horas de marcación continua, o su equivalente en segmentos de tiempo ante inactividad.

Conectividad:

Red (conector RJ-45).

Opcionalmente podrá permitir utilizar PoE (Alimentación a través de Ethernet).

Deberá incluir contacto activable mediante protocolo del tipo TCP/IP, RS485, Wiegand o similar apto para la apertura de puertas.

Deberá incluir todos los accesorios y cables necesarios para su conexión a la red eléctrica y transmisión de datos.

Incluirá todo el software o bibliotecas de software necesarias para el control del dispositivo y el acceso a las imágenes capturadas por el mismo. Deberán proveerse los manuales de uso y la documentación del software o bibliotecas de software provistas, ya sea en papel o en medios digitales.



El software o bibliotecas de software provistos serán aptos para operar en los siguientes sistemas operativos: Microsoft Windows o Linux.

Deberá incluir todos los Kit de Desarrollo de Software (SDK) que sean necesarios para desarrollos de aplicativos de software basados en DLLs, controles ActiveX u otra solución que pueda integrarse fácilmente a entornos de desarrollo.NET, Java, etc.

Para puesto de Enrolamiento (ENROL. HUELLAS USB)

Características:

Conectividad USB 2.0 o superior

Área de escaneo: 15x15 mm (mínimo)

Resolución: 500 DPI (mínimo)

Soporte para: Linux/Windows 7 (32 y 64 bits) y superior

Tipo de escáner Unidactilar.

Escáner de tecnología óptica de huella tipo rolled, no susceptible a descargas electrostáticas (ESD)

Los templates almacenados no deberán incluir imágenes reales de la huella dactilar, sino únicamente los rasgos unívocos (minucias). Cada template, deberá contener al menos 350 bytes de información por cada huella.

El enrolamiento se deberá poder realizar en cualquier dispositivo para control de asistencia, y los templates deberán quedar replicados tanto en el dispositivo, como en la base de datos, de modo de asegurar su resguardo y replicación en caso de ser necesario.

Incluirá todo el software o bibliotecas de software necesarias para el control del dispositivo y el acceso a las imágenes capturadas por el mismo. Deberán proveerse

150



los manuales de uso y la documentación del software o bibliotecas de software provistas, ya sea en papel o en medios digitales.

El software o bibliotecas de software provistos serán aptos para operar en los siguientes sistemas operativos: Microsoft Windows o Linux.

Deberá incluir todos los Kit de Desarrollo de Software (SDK) que sean necesarios para desarrollos de aplicativos de software basados en DLLs, controles ActiveX u otra solución que pueda integrarse fácilmente a entornos de desarrollo.NET, Java, etc.

### **DISPOSITIVOS PARA LA CONFORMACIÓN DE BARRERAS FÍSICAS DE ACCESO**

Se utilizarán dispositivos Nuevos o existentes. En el caso de ser necesario la adaptación de los mismos estará a cargo del Adjudicatario y estarán incluidos todos los accesorios necesarios para su funcionamiento según su tipo.

Se utilizan diferentes tipos y cantidades, dependiendo de las características del acceso y según se indica en planos.

### **CONTROL DE ASCENSORES:**

Se solicita la implementación de control de los ascensores montacargas de los sectores asignados al transporte y circulación de valores, de modo tal que, al subir, sea necesario utilizar su IPB y/o EIP en una lectora instalada en el interior del mismo, para que se habiliten en el panel del ascensor solamente los botones correspondientes a los pisos en los que el agente esté habilitado a subir y/o bajar.

La actividad de IPB y/o EIP relacionada con la selección de pisos deberá quedar registrada dentro de la misma base de datos del sistema de control de accesos que maneja las puertas del edificio.



Los permisos a las IPB y/o EIP sobre los pisos deberán poder gestionarse directamente desde el sistema de control de accesos.

### **CONTROL DE INGRESO VEHICULAR**

Se solicita la provisión e instalación de barreras vehiculares de alta velocidad tipo peaje con sensores anti aplastamiento integrado tipo espira y 2 lectoras de largo alcance (una para entrada y la otra para salida).

El personal que posee cocheras permanentes debe poder ingresar al predio utilizando un dispositivo TAG colocado en el parabrisas de su vehículo que permita agilizar su ingreso. Estos permisos deberán poder gestionarse desde el software provisto.

#### **Barreras vehiculares.**

Tipo:	Automática
Controladora:	Tipo CPU interna.
Alimentación:	220VAC
Consumo:	Menor a 400W

Gabinete: Para exterior, fabricado en chapa de 1,6mm de espesor.

Tiempo de subida: Menor a 2 segundos

Antiaplastamiento: Sensor de presencia vehicular tipo espira integrado.

Características de las lectoras de largo alcance:

Ser aptas para montaje en exterior.

Comunicarse con el panel vía Wiegand.

Rango de lectura de 0-50cm



Tener la capacidad de leer las siguientes tarjetas: Mifare /Iclass HID o IClass HID o equivalentes y capacidad de lectura de TAGs.

### **DISPOSITIVOS CON IMPEDIMENTO FÍSICO PARA PERSONAS:**

Los dispositivos son del tipo molinete mecánico a eje horizontal y permitirán el paso en ambas direcciones con la posibilidad de bloquearlo en uno de los sentidos.

Deberán permitir el paso de una, y solo una, persona por vez.

Deberán indicar a la unidad controladora el sentido del paso de una persona, que previamente ha sido habilitada mediante la presentación de su EIP y/o IPB.

Deberán poseer un sistema de seguridad que impida el giro no autorizado. El mismo podrá ser anulado en caso de emergencia, permitiendo el libre giro del dispositivo o función de aspas colapsables manuales.

Deberán contar con señalización lumínica indicadora del estado de paso habilitado o paso inhabilitado utilizando para ello LEDs bicolores u otra alternativa con igual prestación.

Deberán contar con señalización lumínica indicadora del estado de paso habilitado o paso inhabilitado utilizando para ello LEDs al menos bicolores, indicando para cada color el estado de listo/en funcionamiento, habilitado, y no habilitado.

En caso de falla de energía por tiempo más prolongado que el soportado por la fuente alternativa, se podrán accionar en forma manual.

Molinetes de 3 aspas:

Características

- Tolerancia al trato riguroso alojado en gabinete de doble pie construido en acero inoxidable con refuerzos internos de terminación anticorrosiva.



- Material acero inoxidable AISI 304 de 1.6 mm de espesor y pulido a un acabado N° 4. Estructura metálica mono pieza.
- Mecanismo de alta seguridad y robustez diseñando para uso intenso.
- Diseño elegante y ergonómico.
- A prueba de polvo y derrames de líquidos.
- Acceso unidireccional con sentido de paso configurable.
- Sistema amortiguado.
- Alta resistencia a golpes y vibraciones.
- Libre de mantenimiento.
- Sistema antivandalismo.
- Alimentación en Baja Tensión.
- Aspas: Tres barrales de 500 mm. Tubos de acero inoxidable pulido.
- Mecanismo: rotor siempre libre, rodamientos blindados, bujes auto lubricados, amortiguador hidráulico.
- Sensores de posición del brazo a contacto seco.
- Selenoide de 12 v.
- Señalización de paso y dirección (luz roja – luz verde).
- Espacio para instalación de relojes de proximidad.

#### **CERRADURAS ELÉCTRICAS DE SEGURIDAD.**



Permiten la apertura de puertas bajo el control de las unidades controladoras. Serán activadas mediante un lector de EIP e IPB para el ingreso a las áreas restringidas que se indican en planos y un lector de EIP e IPB o un botón de comando para el egreso de las mismas.

Son del tipo electromagnético y deberán quedar liberadas ante falta de alimentación eléctrica, excepto en aquellos accesos en donde específicamente se indique lo contrario.

Se utilizarán los dispositivos existentes. En el caso de ser necesario la adaptación de los mismos estará a cargo del Adjudicatario y estarán incluidos todos los accesorios necesarios para su funcionamiento según su tipo.

Cerradura Magnética de 600 lbs:

- Multi-voltaje 12/24 vcc
- Sensor de puerta abierta.
- No debe poseer partes móviles.
- Libre de mantenimiento.

### **BRAZO CIERRA PUERTA HIDRÁULICO**

Características:

- Reversible
- Material: Aluminio de alta durabilidad.
- Ajuste de velocidad y dureza.
- Rango de 60 a 100 kgs.



- Vida útil mecánica: 500.000 aperturas
- Velocidad de cierre constante.
- Angulo máximo: 180°
- Ancho máximo de puerta 900-1500 mm.

### **DETECTORES DE APERTURA DE PUERTAS.**

Informarán al sistema de la apertura de las puertas en que se instalen. Cada apertura quedará registrada mediante entradas supervisadas.

### **PUERTA DE CONTROL DE PROVEEDORES, BICICLETAS Y ANTI-PÁNICO**

Características:

- Tolerancia al trato riguroso alojado en gabinete de doble pie construido en acero inoxidable con refuerzos internos de terminación anticorrosiva.
- Material acero inoxidable AISI 304 de 1.6 mm de espesor y pulido a un acabado N° 4.
- Mecanismo de alta seguridad y robustez diseñando para uso intenso.
- A prueba de polvo y derrames de líquidos.
- Alta resistencia a golpes y vibraciones.
- Libre de mantenimiento.
- Acceso unidireccional con sentido de paso configurable.
- Apertura a partir de botón pulsador



### **BUZÓN TRAGA TARJETAS.**

Se utilizan para retener el EIP de visitas al producirse el egreso. La credencial será introducida por el portador en el dispositivo, será leída, retenida y luego de ello la salida será autorizada si corresponde. En caso de tratarse de una tarjeta no válida, la misma deberá ser devuelta automáticamente a través de una ranura o dispositivo para tal fin.

### **TARJETAS DE PROXIMIDAD RFID**

Características:

- Color blanco. Material PVC AB.
- Tecnología ICLASS/Mifare o equivalente
- Frecuencia 125khz o superior

### **DISPOSITIVOS DE ALARMA.**

Se instalarán y configurarán dispositivos de alarma de intensidad regulable, adecuados para ser percibidos por el personal de los puestos de operación local y el usuario, a los efectos de indicar la ocurrencia de un evento de alarma.

Opcionalmente será posible silenciarla, utilizando el software correspondiente, tanto desde el puesto de operador local, así como desde el puesto central y en forma manual desde el puesto de operador local.

### **PROVISIÓN E INSTALACIÓN DE UNIDADES CONTROLADORAS**

Se deberán proveer e instalar la cantidad necesaria de unidades controladoras para que el sistema de control de accesos posea las funcionalidades, performance y disponibilidad solicitada en todos sus puestos locales de control.



Deberán poseer como mínimo capacidad para:

- Recibir instrucciones programadas desde el puesto central de control o desde un terminal local.
- Ejecución de decisiones sobre los puntos de acceso que dependen de él.
- Control y gestión de la totalidad de sus dispositivos periféricos (unidades lectoras, dispositivos de barrera, alarmas, cerraduras etc.).
- Proveer control “antipassback”.
- Supervisar el estado operativo de las líneas y módulos que dependen de él y dar señales de alarma ante intentos de desarme y ante fallas de alimentación.
- Mantener plena funcionalidad en caso de caída del puesto central de control o del enlace con el mismo por el término de 4 hs.
- Almacenar los datos requeridos de no menos de 2500 registros por cada par de lectores que de él dependan, correspondientes a información que se genera por el ingreso o egreso de personas, así como a eventos de alarma.
- Garantizar que el tiempo entre lectura de un EIP e IPB y la indicación de respuesta en cualquiera de los dispositivos indicados en 0 sea menor a 2 segundos, considerando un factor de simultaneidad igual a 1 (uno) para la totalidad de los lectores que dependen de él. Este tiempo será verificado en ensayos de evaluación antes de la recepción definitiva del sistema.
- Inhabilitar, en uno o ambos sentidos, los puntos de acceso que dependen de él, en horarios determinados y programables.
- Almacenar y ejecutar el software requerido para la ejecución de todas sus funciones.

Deberán poseer las siguientes características:



- Unidad basada en microprocesador.
- Se comunicarán con las unidades lectoras utilizando protocolo Wiegand.
- Se comunicarán con el puesto central de control utilizando la red de datos del Organismo.
- En caso de falla deben poder substituirse en forma sencilla y rápida. Las interconexiones serán realizadas por medio de conectores y/o borneras. No debe ser necesario realizar soldaduras para cambiar las unidades concentradoras o controladoras.
- Las entradas y salidas para dispositivos periféricos (sensores, alarmas, etc.) serán provistas en una cantidad que supere al menos en un 20% la cantidad necesaria para el funcionamiento inicial del sistema.

### **CANTIDAD MÍNIMA DE EQUIPAMIENTO EXIGIDO PARA CADA CASINO**

Se indican a continuación las cantidades mínimas exigidas para los sistemas de control de acceso de cada Casino de la presente Licitación. Deberá tenerse en cuenta que los trabajos deben ser completos y asimismo, deberán considerarse incluidos todos los elementos y trabajos necesarios para el correcto funcionamiento, aun cuando no se mencionen explícitamente en pliego o planos.

#### **CASINO CENTRAL**

Puerta 1 Acceso Personal: Instalación de 4 molinetes metálicos de 3 aspas contando con 4 lectores biométricos/tarjetas RFID de entrada y 4 de salida (total 8 lectores)

Puerta 4 Acceso Personal: Instalación de 3 molinetes metálicos de 3 aspas contando con 3 lectores biométricos/tarjetas RFID de entrada y 3 de salida (total 6 lectores)



2 Pilares Barra para proveedores e invitados con un lector biométricos/tarjetas RFID por pilar

2 lectores de BackUp

20 lectores biométricos/tarjetas RFID para control zonas restringidas internas al edificio.

15 Cerradura magnética de 600 lb

2 Pestillo Eléctrico

2 Puertas de control de proveedores, bicicletas y anti-pánico

11 Brazos Cierra Puerta Hidráulico

200 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente

CASINO HERMITAGE, CASINO MIRAMAR, CASINO MONTE HERMOSO, CASINO PINAMAR, CASINO TANDIL

(Cantidades expresadas para cada uno de los edificios)

1 Acceso Personal: Instalación de 1 molinete metálicos de 3 aspas contando con 1 lectores biométricos/tarjetas RFID de entrada y 1 de salida (total 2 lectores)

1 Acceso Proveedores: 1 o 2 lectores biométricos/tarjetas RFID

1 lector de BackUp

20 lectores biométricos/tarjetas RFID para control zonas restringidas internas al edificio

100 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente



## CASINO TIGRE

1 Entrada de Personal: Instalación de 2 molinetes metálicos de 3 aspas contando con 2 lectores biométricos/tarjetas RFID de entrada y 2 de salida (total 4 lectores)

1 Entrada Proveedores: 1 o 2 lectores biométricos/tarjetas RFID

2 lectores BackUp

20 lectores biométricos/tarjetas RDIF para control zonas restringidas internas al edificio

200 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente

Sin perjuicio de las cantidades mencionadas con anterioridad, y teniendo en cuenta que durante la ejecución de las obras en cada Casino pueden surgir necesidades o modificaciones que impacten directamente en el control de acceso y/o áreas restringidas. El Instituto podrá modificar las cantidades exigidas para cada uno de los dispositivos que conforman el Sistema de control de acceso en cada Casino de la presente Licitación. A tal fin, realizará las inspecciones de avance de obra que correspondan y comunicará mediante informe escrito las modificaciones y/o necesidades a ser consideradas e implementadas en lo que refiere al presente capítulo.

## **INSTALACIÓN, CABLEADO, ETIQUETADO E INTERCONEXIÓN DE DISPOSITIVOS**

El Adjudicatario deberá instalar e integrar todos los equipos que se requieran para la correcta operación del sistema de control de acceso ofertado, ajustándose a las necesidades de cada Casino.



Las modificaciones que fueren necesarias para los accesos, puertas, molinetes etc. serán responsabilidad del adjudicatario; debiendo reemplazar cualquier pieza que se rompa producto de la adaptación de los lectores a los diferentes dispositivos que conforman el puesto.

Los detalles de terminación deberán tener un aspecto prolijo, siguiendo las reglas del buen arte y cuidando la estética del lugar.

### **REALIZACIÓN DEL TENDIDO DE CANALIZACIONES.**

En caso de ser necesario, estarán comprendidas en la oferta, los materiales y trabajos para conformar las canalizaciones necesarias para el cableado de red, la alimentación eléctrica y cableado de datos de los dispositivos y todo aquel cableado que fuere necesario realizar para el correcto funcionamiento de los mismos.

Se utilizarán materiales que cumplan con las características que se detallan. En el caso de ser necesario el tendido de otros tipos de canalizaciones para la implementación del proyecto, se especificará y cotizará.

El sistema de canalizaciones deberá ser inspeccionado y aprobado por el INSTITUTO antes de iniciar las tareas de cableado.

Todos los trabajos serán ejecutados de acuerdo a las reglas del buen arte y presentarán, una vez terminados, un aspecto prolijo.

### **CAÑERÍA METÁLICA RÍGIDA PARA INTERIORES.**

Será en todos los casos de caño semipesado fabricado conforme a normas IRAM 2005, hasta 2" nominales (46 mm. de diámetro interior). La medida mínima del caño será 3/4" semipesado (15,4 mm. de diámetro interior) o equivalente.

Se colocarán cajas de pase y derivación.

### **CAJAS DE PASE Y DERIVACIÓN.**



Todas las cajas estarán constituidas por cuerpo y tapa. En instalaciones a la vista estarán prohibidas las cajas de chapa con salidas pre-estampadas, pudiendo ser de aluminio fundido o de chapa lisa, realizándose los agujeros de conexión a cañería que sean necesarios.

Serán de medidas apropiadas a los caños y conductores que lleguen a ellas. Las dimensiones serán fijadas en forma tal que los conductores en su interior tengan un radio de curvatura no menor que el fijado por reglamentaciones para los caños que deban alojarlos.

La medida mínima será no inferior a 6 veces el diámetro nominal del mayor caño que llegue a la caja. El espesor de la chapa será de 1,6 mm. en las cajas de hasta 20 x 20 cm.; 2 mm. En cajas de hasta 40 x 40 cm., y para mayores dimensiones serán de mayor espesor convenientemente reforzado con hierro perfilado.

Las tapas cerrarán correctamente, llevando los tornillos en número y diámetro que aseguren el cierre, ubicados en forma simétrica en todo su contorno, a fin de evitar dificultades en su colocación.

Las cajas serán protegidas contra oxidación mediante pintura anticorrosiva donde la instalación es embutida, o mediante galvanizado por inmersión o zincado donde la instalación sea a la vista.

Todas las canalizaciones nuevas deberán ser aprobadas por el INSTITUTO, previamente al comienzo de las tareas de cableado.

#### CAÑERÍA METÁLICA FLEXIBLE.

Será cañería metálica con recubrimiento de PVC, diámetro mínimo 3/4". Se utilizará en aquellos lugares donde resulte necesario realizar canalizaciones sobre cielorraso.

Se colocarán cajas de pase y derivación.

#### CABLECANAL



El cablecanal será metálico y será utilizado a un 70% máximo de su capacidad, por lo tanto, las dimensiones deberán adaptarse a este requerimiento.

Contará con tratamiento de desengrase, fosfatizado y pasivado que permita una mejor adherencia superficial. Deberá ser pintado con un color similar al utilizado en las paredes o puertas en donde se amurará.

Dispondrá de tapa y protección inferior para evitar desborde de cables.

La fijación del cablecanal deberá realizarse con tornillos y arandelas cada 50 cm.

El sistema de cablecanal contemplará los accesorios necesarios como curva "L", unión "T", puntera, etc.

## **REALIZACIÓN DEL CABLEADO PARA LA ALIMENTACIÓN ELÉCTRICA DE LOS DISPOSITIVOS.**

La alimentación eléctrica de todo el equipamiento del sistema deberá estar soportada de la línea con energía ininterrumpida de 220V - 50Hz. La garantía del equipamiento deberá ser válida para estas características. En caso de requerirse otras tensiones de alimentación, el suministro de las mismas formará parte de la oferta.

Se utilizará la red eléctrica del sistema de control de accesos existente. Dicha red eléctrica deberá ser relevada y, en caso de ser necesario realizar modificaciones en la sección de los conductores o sus protecciones electromagnéticas, las mismas estarán a cargo del Oferente.

El adjudicatario ejecutará la totalidad de los trabajos necesarios para la correcta alimentación eléctrica de la totalidad de equipos a instalar.

Se utilizarán conductores que cumplan con las características especificadas a continuación.

## **CONDUCTORES PARA INSTALACIÓN EN CAÑERÍAS.**



Serán de cobre flexible, con aislación de material plástico antillama, apto para 1000 Vca, con certificado de ensayo en fábrica a 6000 V para cables de hasta 10 mm<sup>2</sup> y a 2500 V, luego de inmersión en agua por 12 horas, para secciones mayores.

Responderán a las normas IRAM 2183 y cumplirán, además, con los requisitos sobre la no propagación de incendios establecidos por las normas IRAM 2289 Cat. "B", exigiéndose en todos los casos los ensayos especificados por las normas.

La manipulación y colocación serán efectuados de manera apropiada, usando únicamente lubricantes aprobados, pudiendo exigir el INSTITUTO que se reponga todo cable que presente signos de violencia o maltrato, ya sea por roce contra boquillas, caños o cajas defectuosas, o por haberse ejercido excesiva tracción al pasarlos dentro de la cañería.

Siempre se mantendrá el mismo color de aislación para fases y neutros de los distintos circuitos trifásicos o monofásicos.

Los colores a utilizar serán los siguientes:

Fases: R, S y T: Marrón, Negro y Rojo, respectivamente.

Neutro: Celeste.

Tierra: Bicolor (Verde - Amarillo). Se prohíbe el uso de cable desnudo.

Serán de la línea SUPERASTIC FLEX de Prysmian o calidad similar.

#### SELECCIÓN DE CONDUCTORES.

La sección de los conductores de los circuitos será seleccionada para no superar una caída de tensión igual al 1% entre el tablero seccional y el último equipo o dispositivo alimentado.

#### IDENTIFICACIÓN.



Cada conductor deberá estar correctamente identificado mediante anillos numeradores, que se ubicaran en el comienzo y en el final de cada tramo del circuito al que correspondan, indicándose el número de circuito al que pertenece.

El primer punto de identificación será la bornera de salida del tablero seccional. La identificación se repetirá en cada caja de pase, en cada centro, en los puntos de conexión a los equipos o dispositivos y en las conexiones a los accesorios de salida.

### **REALIZACIÓN DEL CABLEADO E INTERCONEXIÓN DE LOS DISPOSITIVOS.**

Estarán incluidos en la oferta la totalidad de materiales, accesorios y trabajos necesarios para el cableado e interconexión de todo el sistema de control de accesos.

Estará a cargo del adjudicatario la provisión de equipos, interfaces y todo otro accesorio necesario para interconectar la red del sistema de control de acceso a la red LAN Ethernet existente en el Organismo, utilizando protocolo TCP/IP. Deberá indicar las medidas de seguridad que implementará para impedir accesos no autorizados.

Para la totalidad de los cableados se utilizarán las canalizaciones indicadas en estas especificaciones.

Todos los cableados serán ejecutados atendiendo a las recomendaciones de los estándares y fabricantes según el tipo.

Para ninguno de los cableados se admitirán empalmes.

En cada caja de pase los cables se fijarán utilizando adecuados accesorios.

**CONDUCTORES.**



Para la red de cableado se utilizarán materiales que cumplan con lo indicado por el fabricante del equipamiento. Dichas recomendaciones del fabricante, junto al tipo y dimensionamiento para cada tramo serán presentadas en la oferta.

En el caso de ser necesario el tendido de otros tipos de cables, para la implementación del proyecto, se especificará y cotizará.

Los materiales deberán ser aprobados por el INSTITUTO, previamente a su utilización.

#### IDENTIFICACIÓN.

Todos los cables, cajas de pase y accesorios deberán ser identificados con accesorios adecuados. Los procedimientos de asignación de nombres individualizadores y de documentación deberán ser propuestos por el Oferente y aprobados por la INSTITUTO antes de ponerse en ejecución.

#### **ADECUACIÓN DE LA RED DE SUMINISTRO ELÉCTRICO**

La alimentación eléctrica de las computadoras de los puestos locales de control deberá estar soportada de la línea con energía ininterrumpida de 220V - 50Hz.

Mientras que la alimentación eléctrica de los periscopios para servicios auxiliares de los puestos locales de control deberá estar soportada de la línea de 220V - 50Hz.

Se utilizará la red eléctrica del sistema de control de accesos existente. Dicha red eléctrica deberá ser relevada y, en caso de ser necesario realizar modificaciones en la sección de los conductores o sus protecciones electromagnéticas, las mismas estarán a cargo del Oferente.

Será tarea a cargo del adjudicatario, la provisión, armado, cableado interno e instalación de los periscopios para esos puestos de trabajo.

En cuanto al cableado interno se indica que deben quedar todos sus tomacorrientes conectados en paralelo.



Se utilizarán conductores que cumplan con lo especificado en estas especificaciones.

La sección de los conductores de los circuitos de tomacorrientes para puestos de trabajo, será seleccionada para no superar una caída de tensión igual al 1% entre el tablero seccional y el puesto más alejado del circuito. Para ello deberá tenerse en cuenta una potencia de 500 W por puesto de trabajo y de 2000W para puesto de servicios auxiliares. Asimismo, se considerará un factor de simultaneidad de 0.7 por circuito, y un factor de potencia (Coseno de  $\emptyset$ ) igual 0.85.

#### **CAJAS DE CONEXIÓN.**

Serán del tipo periscopio modular, metálicos de chapa BWG N° 18, pintados y horneados.

Serán periscopios de 4 módulos intercambiables entre sí.

En uno sus laterales dispondrán de un orificio de 1" de diámetro, el cual no deberá tener borde cortante y dispondrá de una tapa plástica roscada.

Poseerán base, tapas, separadores y placas porta accesorios removibles. Estas placas permitirán la instalación de los distintos accesorios de salida (conectores hembra de telecomunicaciones y tomacorrientes eléctricos) descriptos en esta especificación. Las partes removibles serán fijadas por tornillos auto-roscantes templados, zincados, y sin punta.

Cada una de las cajas de conexión deberá ser provista con:

Cuatro tomacorrientes de 2 x 10 A + T que responderán a lo especificado en 0 o en 0 según corresponda.

Un conector modular de ocho posiciones del tipo descrito en 0.



#### TOMACORRIENTES PARA PUESTO DE SERVICIOS AUXILIARES.

Serán simples, de 2 x 10 A + T y cumplirán con la norma IRAM 2071. Constructivamente serán aptos para el accesorio de salida en donde se instalan. Serán tipo Jeluz, con los módulos en color blanco.

#### TOMACORRIENTES PARA PUESTO DE TRABAJO.

Serán simples, de 2 x 10 A + T y cumplirán con la norma IRAM 2071. Constructivamente serán aptos para el accesorio de salida en donde se instalan. Serán tipo Jeluz, con los módulos en color rojo.

#### CONECTORES HEMBRA.

Se utilizarán conectores hembra modulares de ocho posiciones - ocho conductores, tipo RJ45, apto para funcionamiento según categoría 5E.

El cableado de los conectores hembra, responderá a la designación T 568A.

El conector permitirá re-insertar el cable UTP en sus contactos más de diez veces sin que se degrade su performance.

Deberá cumplir con las pruebas de performance de la ANSI/TIA-568-C.2 Categoría 6A/ Clase EA y ISO/IEC 11801: 2002 (últimas revisiones), certificado por Underwritess Laboratories (UL).

Serán SYSTIMAX, FURUKAWA, Simeon o similar calidad y prestación.

#### UPS PARA SOPORTE DE INSTALACIÓN.

Para el caso de los equipos controladores y dispositivos de control instalados, se deberán suministrar el o los Equipos UPS necesarios para dar soporte ante una falla en el suministro eléctrico. Dichos Equipos UPS deberán contar con la potencia adecuada al requerimiento de consumo de los dispositivos a servir y estarán conectados al Tablero Principal de alimentación en una línea individual. Los mismos



deberán contar con una autonomía de al menos 60 (sesenta) minutos de suministro ininterrumpido de energía eléctrica. Deberán detallarse los equipos incluidos en la oferta.

### **CAPACITACIÓN DE PERSONAL PARA OPERACIÓN Y MANTENIMIENTO DEL SISTEMA**

Dentro de los 60 (sesenta) días corridos del inicio de los trabajos, el adjudicatario deberá realizar cursos de capacitación relativos a la tecnología a suministrar, con operación, administración, gestión, explotación, programación y mantenimiento de la misma. Dicha capacitación será dirigida al personal de operación, administración, capacitadores y técnicos del sistema.

En la propuesta debe indicarse el programa y duración de cada curso ofrecido el cual será para no menos de 10 (diez) personas.

El adjudicatario deberá proveer el suministro de guías o manuales de fácil interpretación, para la operación exitosa del sistema, los que estarán redactados en idioma español.

### **MANTENIMIENTO DURANTE PERIODO DE GARANTÍA**

Durante el periodo de garantía, el adjudicatario será responsable de la operación, mantenimiento y servicio de emergencia de la totalidad de las instalaciones de control de accesos, ya sea que fueran provistas o modificadas por él o que ya estuvieran instaladas, y de la realización de todas aquellas tareas necesarias para el correcto funcionamiento del sistema, incluyendo la totalidad de repuestos y trabajos necesarios para mantener el 100% de las prestaciones del sistema tal como fuera instalado, debiéndose sustituir los elementos que resultaran defectuosos y efectuar los arreglos o trabajos necesarios para su correcta operación, por exclusiva cuenta y cargo de la empresa contratista.



El período de garantía será de 2 (dos) años, considerando un uso adecuado de cada elemento, y comienza a regir a partir de la firma del Acta de Recepción Provisoria, debiendo el adjudicatario mantener en concepto de garantía los puestos de control desde su puesta en marcha hasta la firma de dicha Acta.

Para el equipamiento de informática incluido en la oferta de tales como servidores, electrónica de red, el periodo de garantía será de 3 (tres) años y comienza a regir a partir de la firma del Acta de Recepción Provisoria.

Para el mantenimiento durante el período de garantía, los trabajos serán realizados por técnicos certificados por el fabricante de los equipos a instalar y según lo especificado en el presente pliego.

Se deberá incluir en el mantenimiento todos los puntos de operación del sistema, incluyendo las computadoras que se utilizan como terminales de operación y los servidores.

Como parte del mantenimiento, el adjudicatario deberá ofrecer e instalar sin cargo para el Casino, todas las actualizaciones, mejoras o modificaciones del software que ofrezca en el mercado, quedando a criterio del INSTITUTO la aceptación de las mismas.

No deberán incluirse como tareas de soporte bajo contrato:

mantenimientos de base de datos y tareas de backup de las mismas

gestión de altas de ABM o tareas de operación de gestión del sistema adjudicadas a los operadores del sistema (alta y baja de usuarios, enrolamiento, ejecución de reportes posteriores al alta inicial general del sistema).

#### **MANTENIMIENTO PREVENTIVO DURANTE PERIODO DE GARANTÍA.**

Se encarga de la conservación de la totalidad del equipamiento, cableado y software del sistema.



La revisión total del sistema de control de accesos se realizará en forma trimestral.

En dichas visitas se realizarán las rutinas y pruebas, necesarias para el control y comprobación del correcto funcionamiento de la totalidad de las partes que componen el sistema.

En dichas visitas el adjudicatario realizará las rutinas y pruebas necesarias para el control y comprobación de correcto funcionamiento de la totalidad de las partes que componen los sistemas. Como mínimo, deberán estar las tareas de:

Limpieza y normalización de dispositivos, cableados y canalizaciones.

Inspección y cambio de luces indicadoras.

Comprobación del funcionamiento de los dispositivos a nivel hardware y software.

Lubricación de componentes mecánicos que lo requieran.

El plazo para la ejecución de las tareas propias del mantenimiento preventivo no superará las 72h.

## **MANTENIMIENTO CORRECTIVO DURANTE EL PRIMER AÑO**

Incluye sin cargo y en las condiciones establecidas la provisión de repuestos y trabajos necesarios para la solución de fallas producto del uso normal de cualquiera de las partes del sistema.

### **PLAZOS DE MANTENIMIENTO CORRECTIVO.**

Los plazos para la solución de fallas se establecen según el siguiente detalle:

Ante cualquier tipo de falla, el adjudicatario deberá disponer de un servicio de atención telefónica sin cargo, en el horario de operación del Casino, servicio que deberá intentar solucionar remotamente la falla reportada de manera inmediata, siendo necesaria una visita en caso de no lograr solucionar el inconveniente.



Ante una falla que afecte el 50 % o más de la capacidad de registro de personas en un puesto local de control, el plazo de reposición del servicio será como máximo de 12 (doce) horas, contadas a partir de la denuncia de la falla.

Ante las fallas que afecten menos del 50 % de la capacidad de registro de personas en un puesto local de control, el plazo de reposición del servicio será como máximo de 48 (cuarenta y ocho) horas, contadas a partir de la denuncia de la falla.

Ante fallas que afecten el funcionamiento del puesto central de control, el plazo de reposición del servicio será como máximo de 12 (doce) horas, contadas a partir de la denuncia de la falla. Se deberá garantizar la no pérdida de información de entrada y salida cuando los controladores operan en forma autónoma durante este período.

#### **LUGAR PARA LA EJECUCIÓN DE LOS TRABAJOS DE MANTENIMIENTO.**

Las tareas de mantenimiento se realizarán en los lugares en donde se encuentren los sistemas. En caso de excepción, cuando alguna parte deba ser retirada para su reparación en talleres del proveedor o fabricante, éste deberá contar con la expresa autorización del INSTITUTO para su retiro, previo reemplazo de la parte para no afectar la funcionalidad del sistema.

#### **HORARIOS.**

Para el mantenimiento preventivo y correctivo, los horarios de prestación del servicio serán los siguientes.

#### **HORARIO DE MANTENIMIENTO CORRECTIVO y PREVENTIVO.**

Sin restricciones de horarios.



## **RECLAMOS ANTE FALLAS DURANTE EL PERIODO DE GARANTÍA.**

El INSTITUTO comunicará a la prestadora del servicio el reclamo ante cualquier falla, telefónicamente, mediante el envío de un fax, o por correo electrónico, según disponga e informe el prestador para cada uno de los posibles horarios.

Una vez efectuado el reclamo por cualquiera de las vías mencionadas el prestador del servicio, enviara al INSTITUTO la notificación de aceptación del reclamo vía fax, incluyendo en dicha notificación un número consecutivo de reclamo.

## **INFORMES DE MANTENIMIENTO DURANTE EL PERIODO DE GARANTÍA.**

### **INFORME DE MANTENIMIENTO PREVENTIVO.**

Por cada uno de los controles periódicos realizados y para cada uno de los puestos y partes inspeccionadas la prestadora enviará un informe detallado del resultado de la inspección. Dicho informe se presentará en las 48 horas posteriores de ejecutado el mantenimiento.

### **INFORME DE MANTENIMIENTO CORRECTIVO DURANTE EL PERIODO DE GARANTÍA.**

Una vez ejecutado, la prestadora informará detalladamente las causas y acciones tomadas para la solución de la falla reportada. Dicho informe se presentará en las 48 horas posteriores de ejecutado el mantenimiento.

## **PRUEBAS DE FUNCIONAMIENTO**

A fin de comprobar el funcionamiento del sistema provisto y otorgar la recepción de cada puesto de control, se realizará satisfactoriamente un protocolo de pruebas. El adjudicatario deberá contemplar en su oferta la previsión de las pruebas de los siguientes protocolos. No se admitirán costos adicionales a los cotizados para estas pruebas posteriores a la instalación del proyecto.



### **FUNCIONAL, HABILITAR Y REGISTRAR EL INGRESO/ EGRESO DE PERSONAS POR LOS DISTINTOS ACCESOS.**

Se presenta a cada lector una veintena de personas habilitadas, en todos los casos se comprueba la habilitación, señalización y tiempo de lectura. Se verifican las transacciones a las siguientes alarmas, personal no habilitado, intento de ingreso en horario no permitido, intento de egreso sin haber registrado ingreso, intento de ingreso sin haber registrado el egreso. Se mide el tiempo desde que presenta la credencial/ Huella al punto de lectura hasta que se produce la habilitación de ingreso/egreso.

Verificación de señalización lumínica indicadora del estado de paso habilitado o paso inhabilitado.

### **FUNCIONALIDAD DE UNIDADES CONTROLADORAS.**

Se comprueba la generación de alarma cuando hay salida de operación de las líneas de comunicación, la caída del puesto central de control y de enlace con el mismo, falla en el suministro de energía eléctrica. Se verifica alarma intento de desarme o rotura del equipo, mantener plena funcionalidad del puesto en caso de falla por corte de energía, caída de enlace o caída del puesto.

### **FUNCIONAL MÓDULO DE MONITOREO.**

Se comprueba que se monitorea la totalidad de la información que se genera por el ingreso y egreso, alarmas bajo su jurisdicción y se realizan accesos manuales.

### **FUNCIONAL MÓDULO DE VISITA.**

Se comprueba la capacidad de registrar:

Apellido.



Nombre.

DNI.

Foto del visitante, foto del documento y foto de bienes.

Oficina.

Persona a visitar.

Motivo de la visita (seleccionable entre 5 o más opciones).

Tiempo máximo de permanencia

Empresa.

Organización u organismo al que pertenece.

Observaciones (mínimo 255 caracteres).

Se verifica que el módulo permite:

Asignar un EIP a la visita.

Saber si la visita estuvo anteriormente en el edificio y en caso afirmativo presentar en el formulario los datos personales de la visita que se cargaron inicialmente.

Comandar los dispositivos de captura de imágenes.

Ingresar visitas no identificables

ANEXO I- REQUERIMIENTOS DE INTERFASE SIAPE- SISTEMA DE CONTROL DE ACCESO

EXPORTACIÓN DE EVENTOS DE ACCESO



El sistema se ejecutará como servicio del Sistema Operativo y su periodicidad podrá ser configurada según la necesidad del organismo. Se podrá especificar cada cuántos minutos se desea ejecutar el procedimiento de exportación de eventos:

- Cada 15 minutos (recomendada)
- Cada 30 minutos
- Cada hora.

El sistema al ejecutarse exportará todos los accesos registrados en el período de tiempo configurado por el usuario. Cada vez que se ejecuta la exportación se generará un nuevo archivo de texto.

## FORMATO DE DATOS

En todos los casos el formato de datos requerido para incorporar información de las transacciones de Entrada y Salida generadas por el sistema de control de acceso es el siguiente:

### 1. DOCUMENTO:

Formato: alfanumérico (14).

Valores Posibles: TIPO DOC (3): DNI, LC, LE

NUMERO (11): número de documento

Características: Justificado a izquierda y se completan con blancos a derecha y se expresan sin puntos.

Ejemplos: DNI21986758

LC 21986758

DNI3548234



2. FECHA:

Formato: alfanumérico (19) DD-MM-RRRR HH24:MI:SS

Ejemplos: 11-01-2006 13:30:01

11-01-2006 08:20:01

3. TIPO:

Formato: carácter (1):

Valores posibles: E Entrada

S Salida

4. ESTADO:

Formato: numérico (1)

Valores Posibles: 1 fichada válida

8 o 9 fichada indefinida

Cualquier otro número define una fichada no válida

5. APELLIDO:

Formato: carácter (32)

Valores Posibles: es el apellido del agente dueño de la fichada.

Características: justificado a izquierda y completado con blanco a derecha.

### OPCIONES DE ENVÍO

Se puede enviar la información de las transacciones generadas por el sistema de control de acceso de la siguiente manera:

#### Archivo Plano



- Nombre: debe respetar el siguiente formato “**cod\_organismo(3 posiciones)\_Fichadas\_aammdd\_hhmm.txt**”. (de ahora en más Fichadas.txt)

**Ejemplo:** “070\_Fichadas\_170713\_1059.txt”.

- Formato de Línea:
  - Formato: debe respetar lo descrito en la zona FORMATO DE DATOS
  - Los campos van separados por coma. iii. El tamaño es de 72 caracteres

### WebService

El mismo deberá proveer con el formato con antelación descrito, la información generada en un período de tiempo a convenir.

### MÉTODO DE ENVÍO Y RECEPCIÓN

Los métodos son los siguientes:

#### Para archivos planos o de texto

#### Manual

Ingresando a <https://portal.rhh.gba.gov.ar/fichadas/upload.html> se obtiene la

Transferencia de Archivos de Fichadas

Usuario:   
Ingrese el nombre de usuario.

Clave:

Archivo a Transferir:  No se ha seleccionado ningún archivo.  
Presione el botón para seleccionar el archivo a transferir.

Nombre de Archivo en el destino:   
Debe ingresar el nombre completo, con el formato "Fichadas###.txt" donde los ### corresponden al código de organismo.



siguiente página

Se coloca el usuario y pass (se deben solicitar a la mesa de Ayuda de Siape), el archivo plano a subir y luego presionar el botón “Transferir Archivo”.

### Transferencia de archivos a través de script

Se genera un archivo de ejecución en segundo plano para disparar el proceso de envío de fichadas a intervalos de tiempo a convenir de acuerdo a la necesidad del Organismo en cuestión.

A continuación, se detalla un ejemplo para un ambiente Windows:

#### 1. Crear los directorios

```
c:\Fichadas c:\Fichadas\Logs
```

2. Programar la salida del sistema de fichadas para que guarde los datos en el archivo c:\Fichadas\Fichadas.txt

3. Programar una tarea (en Windows) para que ejecute el script (p.ej.

```
c:\wget_gob\enviar_fichadas.bat) con la frecuencia requerida
```

Ejemplo de script que sube las fichadas

```
@ echo off
```

```
rem Envía las fichadas al server de Gobernación
```

```
if not exist C:\Fichadas\Fichadas.txt goto SIN_ARCHIVO start sube
```

```
goto SALIR
```

```
:SIN_ARCHIVO
```

```
date /T >> log.txt time /T >> log.txt
```



echo ' - No se encontro archivo para enviar' >> log.txt

:SALIR

El script se fija si existe el archivo c:\Fichadas\Fichadas.txt si lo encuentra, lo sube automáticamente al servidor.

IMPORTANTE: escribe Logs de resultado en c:\Fichadas\Logs por lo tanto se debería guardar el archivo de fichadas como "c:\Fichadas\Fichadas.txt"

### **Transferencia de archivos a través de sFTP (Recomendado)**

Se asignará una carpeta en nuestro servidor sFTP, con usuario y contraseña de acceso. En dicha carpeta el organismo dejará disponible los archivos de fichadas que luego serán procesadas de manera automática.

Los archivos transferidos deben ser generados bajo charset utf-8.

IMPORTANTE: Solo podrán utilizar este método los organismos cuyos servidores pertenezcan a la red provincial. La habilitación es vía IP, las cuales serán solicitadas oportunamente.

### **Transferencia de archivos a través de un Webservice**

#### **De Fichadas**

El sistema de control de acceso deberá proveer un WS que brinde información de las transacciones de Entrada y Salida con el formato antes descripto. Desde SIAPE se desarrollará un cliente para consumir dicho WS. El mismo se ejecutará de manera automática en un determinado período de tiempo según la necesidad del Organismo que implemente el sistema de Control de acceso

#### **De Restricción de Acceso**



SIAPE podrá proveer de información de los agentes que, por distintas condiciones a acordar con el organismo, no estarán habilitados a ingresar al edificio en cuestión en un período de tiempo.

#### **ARTICULO 11°: IMPLEMENTACIÓN DE SISTEMA POR COBRO DE ENTRADAS DE INGRESO A CASINOS.**

El adjudicatario deberá colaborar y cooperar con los Municipios -en donde se encuentren los respectivos Casinos adjudicados- y con el INSTITUTO con la percepción, fiscalización y control del arancel de ingreso y permanencia a los casinos, de conformidad con la modificación introducida por el art. 8° bis de la Ley N° 11.018, que fuera incorporado por el art. 194° de la Ley 14.880, en cumplimiento con los términos y condiciones que se acuerden en los respectivos convenios, tal como lo prevé la citada norma.

#### **ARTICULO 12°: PROVISION Y MANTENIMIENTO DE SERVICIOS DE LIMPIEZA, EMERGENCIAS Y SEGURIDAD.**

A) Prestación de un servicio permanente de limpieza integral con insumos y su mantenimiento. La provisión del servicio de limpieza general del espacio tanto de uso público como las dependencias internas de los Casinos objeto de la presente licitación, y la provisión del servicio de limpieza de la sala de juegos durante el horario de funcionamiento de la misma (servicio de escobistas), incluyendo la indumentaria necesaria para el personal de cada sala y la provisión de los elementos necesarios para realizar dicha tarea.

B) Provisión por abono mensual de un servicio de emergencias médicas área protegida. Se cubrirá la atención inmediata y posterior traslado, de resultar necesario, a la Institución Asistencial que la dirección del establecimiento indique, a los fines de continuar con la atención definitiva del paciente. Este Sistema cubrirá por medio de las coberturas medicas por ambulancia, la atención de emergencias y



urgencias médicas, según normativa vigentes y para la totalidad de las patologías que se pudieren producir, incluyendo a todas las personas que se encuentren dentro de los límites de los casinos a licitarse, zona que se denominará AREA PROTEGIDA, contando con el equipamiento, medicamentos, profesionales médicos y enfermeros capacitados en RCP (Reanimación Cardiopulmonar) avanzada, con más la inclusión de todo el material e insumos que se utilicen en los respectivos actos médicos. La asistencia será brindada a requerimiento de las autoridades de los casinos o persona que tomare conocimiento de la Emergencia y/o urgencia y comprenderá la atención médica que requerirá la persona en el área delimitada sin distinción de edad ni actividad en que se produce la misma, y en caso que el paciente deba ser trasladado a un centro de mayor complejidad, la empresa lo hará hacia el lugar preestablecido por el enfermo, familiar o facultativos intervinientes. El servicio a prestar no será limitado en el número de requerimientos. La Empresa a contratar deberá contar todos los seguros que estipula la ley.

C) Provisión, mantenimiento y renovación de sistemas de detección temprana de incendio. Sistemas de agua. Los sistemas comprendidos en este ítem deberán estar en acuerdo al marco regulatorio que se encuentra comprendido por la Resolución N° 189/2011 del INSTITUTO, en concordancia con lo establecido por el Decreto N° 12/2005 del Poder Ejecutivo Provincial.-

#### 1. Sistema de Detección temprana de incendio

Central de Incendio Analógica Inteligente, con capacidad para Mil (1000) Detectores, circuito de Dos (2) Lazos.-

Detectores Térmicos o Fotoeléctricos de Humo a determinar en obra, inteligentes direccionables.-

Estrobos (con Sirena y Destelladores) con módulos direccionables independientes.-

Pulsadores o Activadores de Incendio con módulos direccionables independientes.-

PC rackeable de 19" con programa de detección de los eventos aplicados sobre planos del complejo, con almacenamiento en histórico de eventos.-



El número de componentes se deberá determinar Casino por Casino, en acuerdo al alcance por superficie y la distribución de los ambientes donde se deben instalar.-

La cobertura deberá alcanzar a la totalidad de la superficie de cada Complejo.-

## 2. Sistema de Extinción Manual. Extintores

Extintores ABC de 5 Kgrs cada uno.-

Extintores Hc Fc de 5 Kgrs cada uno.-

Extintor AGUA de 10 Litros.-

Extintor CO2 de 5 Kgrs.-

Extintores ABCK de 6 Litros cada uno.-

Extintores ABC de 25 Kgrs cada uno.-

Estaciones con Doble Balde de Arena.-

## 3. Sistema de Agua

### Hidrantes Interiores

Desde el Troncal de Ø 6" proveniente desde la sala de Bombas se derivará una cañería de Ø4" la cual se distribuirá sobre cielorraso, protegiendo con la cantidad de Hidrantes necesarios (aproximadamente 14), previendo el montaje de 1 válvula mariposa de Ø4", que faciliten el mantenimiento de la red, sin dejar sin agua al resto de la instalación.

Este sistema alimentará a los Hidrantes ubicados estratégicamente en el interior y protegerá todas las áreas del Complejo.

Cada Hidrante estará compuesto por los siguientes elementos y responderán a las siguientes características:

1(una) Válvula de Incendio tipo teatro Ø1 3/4" construida en bronce, con salida a 45°, con su correspondiente tapa y cadena de seguridad.



1(una) Lanza Ø1 3/4", construidas en cobre y bronce con boquilla regulable tipo (chorro pleno-niebla) de accionamiento por rosca.

1(una) Llave para ajustar uniones para Ø1 3/4".

1(un) Tramo de manguera Ø1 3/4" x 25 mts de longitud con sus correspondientes uniones de bronce mandriladas, fabricadas totalmente en material sintético y revestimiento interior de látex.

1(un) Gabinete para alojar mangueras y lanza, construido en chapa de hierro, con puerta de vidrio (p/áreas de servicio), soporte para manguera y lanza.

Los gabinetes para las áreas públicas, estará construido en Acero Inoxidable, con puerta de Vidrio, y filetes de Acero Inoxidable.

Hidrantes (Hx) a instalarse conforme superficie del Complejo:

4. Sistema de Sprinklers en Casino, Circulación y áreas de Servicio Componen este Sistema aproximadamente (número en acuerdo a cada Casino alcanzado por la presente licitación) sprinklers, los mismos estarán comandados por una Estación de Control y Alarma Ø 4" con la siguiente clasificación de riesgo:

Casino, Circulación, Áreas Públicas:

RIESGO: Ligero

MODELO DE SPRINKLER: Tipo Quick Response

TIPO DE SPRINKLER: Pendiente y de Pared

Los rociadores serán del tipo Pendiente (p/Cielorraso) y cumplirán con las siguientes características:

Posición: Pendiente

Orificio de descarga: 1/2" (12mm)

Factor K: 5,6



Material:	Bronce
Temperatura:	155°F (68°C)
Rosca de conexión:	½ " NPT
Máxima presión de trabajo:	50 psi
Marca:	Reliable Sprinkler o Marca Similar
Áreas de Servicio Casino:	
RIESGO:	Ordinario Grupo 1
MODELO DE SPRINKLER:	Tipo Quick Response
TIPO DE SPRINKLER:	De Pie / Pendiente

Los rociadores serán del tipo de Pie y/o Pendiente y cumplirán con las siguientes características:

Posición:	De Pie / Pendiente
Orificio de descarga:	1/2" (12mm)
Factor K:	5,6
Material:	Bronce
Temperatura:	155°F (68°C)
Rosca de conexión:	½ " NPT
Máxima presión de trabajo:	50 psi
Marca:	Reliable Sprinkler o Marca Similar

OBSERVACIONES:



- 1.- Los Equipos propuestos y su distribución, se encuentran sujetos en su número al cálculo de la carga de fuego que se realice una vez concluidas las obras.-
- 2.- Se detallarán en los planos los sectores que se destinarán para las Calderas, reservas de agua y las Bombas Impulsoras de Agua.-
- 3.- Con relación a lo propuesto para el rubro detección, el número de Detectores y ubicación en los Entretechos, quedará sujeto a definición en obra, previendo no obstante que la Central de Incendio señalada tiene la capacidad suficiente para incorporar lo que se determine, entendiéndose que cada detector deberá cubrir una superficie limpia y sin divisiones de entre 16 y 20 metros cuadrados cada uno.-
- 4.- Los Sprinklers no deberán instalarse en superficies con equipos electrónicos (Sala de Monitoreo, Sistemas, Sala de Máquinas, Laboratorio y áreas con Valores en efectivo), para lo cual, se implementarán sistemas de extinción manual con químicos que no dañen los equipos.-
- 5.- En las áreas de valores instalar sprinklers pero con un sistema de pre acción.
4. Provisión y Mantenimiento por abono mensual de Sistemas de Alarma contra Incendio y Robo.

Componentes:

Equipo de Abonado Policial.-

Centrales de Alarma modelo de 8 particiones cada una.-

Sensores Infrarrojos de movimientos de doble tecnología con anti enmascaramiento incluyendo soportes.-

Teclados Alfanuméricos para manejar todas las zonas (incluidos Bóvedas y Recintos de Tesoros) desde un solo lugar a designar.

Teclados Alfanuméricos para Bóvedas y Recintos de Tesoros.-

Avisadores Manuales de robo con aviso policial.-



Avisadores de robo con retención para aviso local.

Receptores Inalámbricos.

Avisadores Manuales inalámbricos portátiles.

Detectores Magnéticos modelo.

1 UPS con batería con capacidad para soportar doce 12 horas.-

Para Monitoreo en Sala de Control:

PC Computadora para aplicaciones técnicas especiales con Monitor Color, Teclado, Mouse y Software para control de eventos en forma automática e inmediata de producido los mismos, con histórico de los anteriores e identificación de hora, fecha y periférico activado; señal de alarma por daño de cualquier parte del sistema, corte de señal, falta de 220v, desactivación o falla del equipo, falta de señal a Policía; con monitoreo secuencial permanente, con señal de aviso de robo e incendio.

El programa deberá contener planos del establecimiento con ubicación de los periféricos, de manera tal que al producirse una señal de alarma, se pueda acceder a la ubicación del mismo por pantalla indicativa.-

Placas Bap (para el monitoreo TCP/IP).-

Impresora.-

Rack para PC, Monitor, Teclado, Mouse e Impresora.-

Condiciones Generales:

Los equipos deben ser provistos por distribuidores oficiales de las marcas ofrecidas, contando con el respaldo de servicio técnico con Laboratorios certificados y autorizados por el fabricante como condición indispensable de garantía. Al efecto se deberán acompañar las presentaciones con los Certificados que habiliten estas condiciones.-

La totalidad de los Equipos deberán entregarse con sus respectivos Softwares de

188



gestión con sus Licencias autorizadas.-

Será la Autoridad de Aplicación – el INSTITUTO – quien determinará a través del personal de Seguridad de los Casinos provinciales, la configuración y número de los equipos componentes de los Sistemas de Seguridad y homologará los mismos conforme sus prestaciones; todo en acuerdo a la planificación y estrategias de seguridad que éste determine.-

5. Servicio Policía Adicional (POLAD): El servicio de Seguridad de los Casinos objeto de la presente licitación, deberá ser brindado por personal de la Policía de la Provincia de Buenos Aires, mediante el Servicio de Policía Adicional (POLAD) en los términos de la Ley 13.942, debiendo absorber el adjudicatario el costo que ello implique.

6. Servicio y Mantenimiento de ascensores. Para el caso de aquellos Casinos que requieran Servicio y Conservación de Ascensores, se exigirá: limpieza, lubricación, engrase e inspección las instalaciones de los ascensores, mínimo una vez cada treinta (30) días. Se incluyen los ajustes menores que se consideren necesarios y la reposición sin cargo de fusibles en controles y tableros, como así también el suministro de los materiales necesarios para el funcionamiento como aceite, grasa, estopa, esmeril, etc.

La Empresa deberá atender los reclamos de cualquier tipo, en días hábiles, en el horario de 8:00 a 20:00 hs contando con la asistencia personal técnico dentro de un plazo de 36 hs. Asimismo la Empresa deberá mantener una guardia durante las 24 hs. los 365 días del año, entendiéndose por emergencia gente encerrada, ascensores parados o motivo de peligro para usuario y/o instalaciones.

En los casos que fuera necesario efectuar el cambio de repuestos por motivo de rotura, quemadura o desgaste de los existentes, la empresa garantizará la provisión del repuesto respectivo, a fin de permitir su reparación y un correctivo funcionamiento de la máquina.



### **ARTICULO 13º: PROVISION DE SERVICIOS COMPLEMENTARIOS:**

- Provisión, mantenimiento y renovación de equipos de comunicación con alcance interno y externo en la periferia del establecimiento, con un mínimo de cuatro canales de banda encriptada en UHF y accesorios.
- Equipos Portátiles de Comunicación.
- Baterías adicionales de alta duración, sin efecto memoria.-
- Cargadores de Baterías.-
- Transformadores para cargadores de baterías.-
- Kits de audio vox color negro.-
- La adquisición debe incluir la Programación de los Equipos en Banda UHF en un número de cuatro (4) canales.-
- Instalación de central telefónica con líneas internas y externas conforme el requerimiento y necesidades del INSTITUTO.

**NOTA:** Componentes sujetos a ampliaciones por definición del proyecto.-

#### **Condiciones Generales:**

Los equipos deben ser provistos por distribuidores oficiales de las marcas ofrecidas, contando con el respaldo de servicio técnico con Laboratorios certificados y autorizados por el fabricante como condición indispensable de garantía. Al efecto se deberán acompañar las presentaciones con los Certificados que habiliten estas condiciones.-

Los equipos deberán ser de primera línea, diseñados y fabricados en origen.

La totalidad de los Equipos deberán entregarse con sus respectivos Software de gestión con sus Licencias autorizadas.-

a) Provisión y Renovación cada dos años de uniformes de trabajo para el personal



operativo. Los uniformes del personal operativo de los casinos deberán comprender a personal masculino y femenino, conforme especificaciones y cantidades por función y características que indicará el personal técnico de casino dependiente del INSTITUTO. El adjudicatario deberá suministrar la renovación de los uniformes cada dos (2) años, sin excepción, los que deberán ser idénticos a los provistos inicialmente, sin uso y de similares características y calidad, para la totalidad del personal comprendido. Además, el adjudicatario deberá poseer un stock de reposición, idéntico al provisto inicialmente, sin uso y de similares características y calidad para recambios antes del tiempo de renovación, solamente cuando: a) Se denuncie la rotura de las prendas, para cuyo caso el empleado deberá acompañar el pedido entregando la prenda con inconvenientes; b) En el caso de pérdidas, para cuyo caso deberá acompañar la denuncia pertinente ante el Departamento Personal del Casino; c) En el caso de cambios de función, para lo cual deberá acompañarse nota de la Jefatura de Juego de Casinos que certifique esta situación. Las prendas alcanzadas, sin perjuicio de las especificaciones y modelos que determine el personal técnico de Casinos, será: Ambos - Chalecos - Pantalones - Camisas - Chaquetas - Moños - Corbatas - Pañuelos "Carre" – Zapatos.

b) Provisión, instalación, mantenimiento y renovación de un sistema central de suministro de aire frío/calor para todas las áreas de los casinos. El inmueble deberá contar con el servicio de calefacción y aire acondicionado integral, con capacidad suficiente para climatizar las salas de juegos, las dependencias internas y sistema de ventilación. Asimismo deberá prestar el servicio de mantenimiento de los mismos a efectos de asegurar su normal y óptimo funcionamiento, conforme las indicaciones requeridas por el INSTITUTO.

c) Sistema de renovación de aire y extracción de humo. El prestador deberá instalar a su costo un sistema de renovación de aire y extracción de humo en las salas de juego y en todas las áreas administrativas y complementarias, que posean la capacidad suficiente que permita una correcta evacuación de humo y odorización de ambientes, que garanticen las exigencias de la Ley N° 13.894; procurando que el nivel sonoro, tanto del ventilador como del aire que circula por el conducto sean



mínimos, de manera que el ambiente que se respira no sea perjudicial para la salud. El prestador deberá garantizar un servicio técnico permanente que asegure el adecuado funcionamiento del sistema instalado que cumpla con todas las pautas que exige la autoridad provincial ambiental competente en la materia.

En la Superficie de la Sala de Racks y UPS se deberá contar Con Aire Acondicionado permanente con temperatura entre 18° y 20°.-

El oferente deberá proveer la solución técnica para la renovación del aire y la extracción del humo, la que serán evaluados por nuestra comisión técnica.

d) Provisión, instalación, mantenimiento de un Sistema de Iluminación con insumos necesarios de recambio. La provisión, instalación, y con insumos necesarios de recambio y renovación de un sistema de iluminación que garantice una iluminación mínima de 300 lux en áreas con control por Cámaras y la necesaria en los demás sectores y una red de iluminación de emergencia que garanticen una iluminación en los porcentajes que se establecen en el presente apartado con relación a todos los Casinos alcanzados por la presente licitación.

#### Iluminación requerida en Sala de Juegos:

No inferior a Trescientos (300) Lux.-

Las luminarias para Mesas y Cajas deberán permitir graduar su intensidad y potencia para evitar los reflejos.-

#### Alimentación de Energía de Emergencia

Deberá contemplarse la instalación de una red de energía de emergencia con luminarias independientes, alimentadas por UPS con Baterías para una (1) hora, según el siguiente esquema:

- 40 % para las Salas de Juegos y Sectores Internos



- 100% para Sectores de Cajas y Tesoros
- 100% para Pasillos Técnicos, Salidas y Escaleras de Emergencia
- 100% para Sala de Cómputos y Racks
- 100% para Salas de Monitoreo y Racks

e) Provisión, instalación y mantenimiento de un sistema de alimentación ininterrumpida (ups) con insumos necesarios de recambio. Provisión, instalación, y mantenimiento de un sistema de alimentación ininterrumpida (UPS) el cual deberá ser de primera marca con placa de red, cuya autonomía mínima para alimentar los equipos instalados deberá ser de mínimo una hora. La batería deberá cumplir los siguientes requisitos: Batería plomo-acido, de libre mantenimiento con electrolito suspendido; Forma de onda de salida: Senoidal; Tiempo de recarga: 3 horas; Compatible con protocolos de APC; Soporte de monitoreo y gestión vía ethernet.

f) Provisión, instalación y mantenimiento de un grupo electrógeno con insumos necesarios. La provisión, instalación y mantenimiento de un grupo electrógeno con insumos necesarios, que deberá garantizar un mínimo de 12 (doce) horas de suministro de energía. La potencia de KVA del equipo estará ligada al consumo que surja de la propuesta que realice el oferente, la que será evaluada por la comisión técnica del INSTITUTO.

#### **ARTICULO 14°. PROVISION DE SERVICIOS DE RESTAURANTES, BARES Y CONFITERIAS.**

14.1. El Adjudicatario deberá instalar un restaurante, bar y confitería, en el sector o espacio destinado a las Sala de casinos y máquinas, para el público asistente y para el personal.

Los servicios de bar, confitería, restaurante, para el público asistente y sala de descanso, y confitería para el personal, serán de primera calidad y sus precios no podrán exceder a aquellos que rijan en establecimientos análogos y de similar

193



categoría, con excepción de los precios que regirán para el bar de la Sala de Descanso del personal. En este caso los precios se reducirán en un cuarenta (40%) por ciento respecto de los establecidos para la Sala de Juegos.

La lista de precios en ambos casos deberá ser remitida al "INSTITUTO".

El adjudicatario podrá habilitar, administrar y explotar otros bares y/o confiterías que estime conveniente allí instalar, siempre y cuando su ubicación no interfiera con el normal desarrollo de las mencionadas salas. Para ello el adjudicatario deberá requerir previa autorización al INSTITUTO, el que solo podrá oponerse a la ubicación de dicho bar y/o confitería en el supuesto que la misma comprometa el normal funcionamiento del Casino y de las máquinas. La eventual habilitación de bares y/o confiterías que se hace referencia en este párrafo no generará alquiler, canon o cualquier otra denominación a favor del INSTITUTO.

Se deja expresamente aclarado que el INSTITUTO no garantiza la rentabilidad de las explotaciones que explote el adjudicatario.

14.2. A su vez, el adjudicatario deberá y estará facultado para la realización de eventos y de espectáculos de entretenimiento.

#### **ARTICULO 15°. PROVISIÓN Y RENOVACIÓN DEL MOBILIARIO DE LAS DEPENDENCIAS INTERNAS Y COFRES PARA LOS VESTUARIOS DEL PERSONAL.**

El mobiliario de las oficinas está conformado por Mesas de escritorio, sillas, Gabinetes.-

Escritorios de madera enchapados de 1.20 x 0.70 mtrs. con cajonera.-

Gabinetes de madera enchapados de 0.90 x 0.45 x 1.50 mtrs.-

Silla cantidad 4 por Oficina, tapizadas, reforzadas y tapizadas en eco cuero lavable.-



Las Oficinas de Contabilidad y Finanzas (1 por cada Casino) llevan 2 escritorios; 6 sillas y 2 Gabinetes por cada una.-

Cofres (Lockers) de metal reforzados con puertas con traba/candados individual para cada puerta. Cantidad en función de los agentes de juego y administrativos que se detallaron para la indumentaria de cada Casino.-

#### **ARTICULO 16°. MANTENIMIENTO INTEGRAL DE LA TOTALIDAD DE LOS INMUEBLES OBJETO DE LA PRESENTE LICITACIÓN.**

El mantenimiento edilicio debe ser preventivo y correctivo de todas las instalaciones. En caso de inutilidad total y/o fin de la vida útil de/l materiales o componentes que resulten comprendidos se deberá renovar de los mismos.

#### **ARTICULO 17°. EN MATERIA DE INFRAESTRUCTURA:**

Se requerirá al adjudicatario, la remodelación, construcción y/o cesión de espacios destinados al funcionamiento de los Casinos objeto de la presente Licitación. En ambos casos, el INSTITUTO acordará con el adjudicatario, un plan de seguimiento y avance de obra, con el objetivo de exigir el cumplimiento de los plazos previstos para la finalización de cada proyecto, conforme Artículo 18° Ap. 1), 2), 3), 4), 5) y Artículo 19° Ap. 1) y 2), Capítulo III de Condiciones Técnicas.

- Los inmuebles que el adjudicatario deberá proveer para la construcción y/o cesión, y funcionamiento de los Casinos de Monte Hermoso, Pinamar, Tigre, Miramar y Tandil, además de las especificaciones que se exigen para cada casino en particular, deberán contener:
- Un (1) Núcleo de Cajas
- Tesoro y Ante-Tesoro de Fichas con Cajas Internas



- Tesoro y Ante-Tesoro de Efectivo con Cajas Internas
- Sala de Conteo de Drop
- Depósito Interno de Tesoros
- Accesos
- Sala de Sistemas para el INSTITUTO
- Sala de Sistemas para la Empresa
- Pasillos Internos
- Ingreso Camión de Caudales
- Laboratorio de Máquinas
- Depósito de Máquinas
- Depósito de Material de Juego
- Áreas Administrativas para la Empresa
- Áreas Administrativas para el INSTITUTO
- Salas de Atención Médica (una por planta) aledañas a Salidas de Emergencia
- Oficinas para Procedimientos de Seguridad (una por planta) aledañas a Salidas de Emergencia
- Baños y Vestuarios Masculinos
- Baños y Vestuarios Femeninos
- Servicios gastronómicos internos y externos
- Guardarropas para Público en Sala de Máquinas y Sala de Mesas
- Centro de Atención de Clientes



- Sala de Espectáculos
- Salas de Venta de Regalos y Suvenires

### **Condiciones Edilicias para las Salas de Juegos – Sectores de Cajas y Tesoros**

Resulta necesario en este tipo de complejos que los cielorrasos sean dinámicos, en paneles simétricos o placas removibles y/o de condiciones que permitan variar las posiciones de lo instalado sobre ellos, sin producirse inconvenientes.-

Mismo criterio se deberá seguir en los entretechos que deberán permitir el mantenimiento por dentro de los mismos.-

Traslado del cableado por bandejas para corrientes débiles y en el caso de Incendio por cañerías MOP por separado.-

Los Pisos deberán ser del tipo Técnico en paneles con capacidad de resistencia acorde al alto tránsito al que serán sometidos.-

Los áreas de Cajas, Ante-Tesoros, Tesoros, Pasillos Técnicos y área de entrega (recinto para el Camión de Caudales y sector de recepción) y traslado de valores hacia el exterior, deberán encontrarse interconectados en superficies independientes de circulación por estrictas razones de seguridad.-

#### **Altura necesaria de Cielorrasos y Entretechos:**

En Cielorrasos no inferior a Cuatro (4.00) Metros, sin interferencias y/o sobre techos intermedios que obstaculicen la correcta visión. La posición de las Cámaras Fijas o Móviles y las luminarias es elemental para una adecuada prestación.-

En los Entretechos una altura no inferior a los Dos (2) metros de altura.-

Se detallará para cada Casino en particular, el tipo de obra requerido.



- Los inmuebles que el INSTITUTO proveerá para el funcionamiento del Casino Central de Mar del Plata y del Casino Anexo III de Mar del Plata (Hotel Hermitage), deberán ser reacondicionados conforme las especificaciones que se detallan en el apartado correspondiente para cada uno de ellos.

## **ARTICULO 18º: CASINOS A CONSTRUIR**

### **1.- CASINO TANDIL**

#### **ESPACIO**

El adjudicatario, deberá proveer un espacio físico apto para la construcción y/o cesión, y funcionamiento del Casino de Tandil, el cual deberá contemplar como mínimo una superficie de un mil cien (1100) metros cuadrados para uso integral de la sala de juegos, y seiscientos sesenta (660) metros cuadrados para dependencias internas operativas, administrativas, de descanso, vestuarios, baños, depósitos y laboratorio. El plazo previsto para la finalización de dicha obra, será como máximo de veinticuatro (24) meses.

El casino deberá contemplar, los siguientes requerimientos:

**-Slots:** Doscientos treinta y dos (232)

**-Mesas:** Diecisiete (17) mesas de juegos de Paño, las que deberán contener:

- Ocho (8) Mesas de Ruleta Americana
- Dos (2) Mesas de Ruleta Francesa
- Dos (2) Mesas de Punto y Banca
- Dos (2) Mesas de Black Jack
- Dos (2) Mesas de Poker



- Una (1) Mesa grande de Craps

Paños de juego: Se calcula en base doble por número de mesas a los efectos de tener stock de reposición.

La distribución de las Mesas de Paño será realizada de acuerdo al criterio adoptado por el el INSTITUTO.

**SECTOR CASINO:** El espacio cuyo uso se cede, deberá poseer:

**Superficies en distribución:**

- Cuatrocientos sesenta (**460 M2**) Metros Cuadrados para Máquinas
- Quinientos treinta (**530 M2**) Metros Cuadrados para Mesas
- Ciento diez (**110 M2**) Metros Cuadrados para restaurantes y afines

**Superficie para áreas del Circuito de Valores:**

- Sector de Cajas de 7m x 4m = **28 M2**
- Ante-tesoro de Fichas con Cajas Internas y Oficina de 6m x 5m = **30 M2**
- Tesoro de Fichas de 3m x 3m = **9 M2**
- Ante-tesoro de Efectivo con Cajas Internas y Oficina de 4m x 5m = **20 M2**
- Tesoro de Efectivo de 3m x 3m = **9 M2**
- Sala de Conteo de Drop de 8m x 5m = **40 M2**
- Pasillos de **1.20 m de ancho**

**Superficie de la Sala de Monitores del INSTITUTO**

- Una Sala de Control



- Oficina y Sala de Edición
- Descanso para personal
- Baños Internos

**Superficie: 6m x 5m = 30 M2**

#### **Superficie de la Sala de Monitores de la Empresa**

Una Sala de Control

Oficina y Sala de Edición

**Superficie: 4 m x 5 m = 20 M2**

#### **Superficie de Áreas Administrativas INSTITUTO y Empresa**

Áreas de Gerencias, Subgerencias, Contabilidad, Cabina, Sistemas, Atención al Cliente, Servicio Médico, Seguridad, Guardarropas, Limpieza, Depósito y Laboratorio = **360 M2**

#### **Superficie de la Sala de Baños (Público y Personal) – Vestuarios y Descanso del personal**

Incluyen personal de la Empresa, del INSTITUTO y para el público, en tres (3) Baterías por separado para masculinos y femeninos. Más área destinada al Descanso de Personal. Oficinas Gremiales

Total: **350 M2**

#### **Contadoras y clasificadoras de billetes:**

- Dos (2) Glory UW 500 (4 bolsillos de proceso + 2 de rechazo de los cuales uno es para billetes dudosos y otros para errores mecánicos), o similar de igual o mejor prestación. Equipo que lee TITO.



- Seis (6) Glory GFB 801, o similar de igual o mejor prestación.
- Dos (2) Glory GFS 120 (equipo de 2 bolsillos, con tapa anti polvo en el bolsillo de proceso), o similar de igual o mejor prestación.
- Tres (3) Lámparas Detectoras de Billetes Falsos marca Royal ND 140 luz UV + luz blanca, o similar de igual o mejor prestación.
- Una (1) Enfajadora G&D BB 40 (solo para uso continuo heavy duty), o similar de igual o mejor prestación.

#### Cámaras CCTV:

El casino deberá contemplar, como mínimo:

- Veintitres (23) Domos
- Cuarenta y nueve (49) Cámaras Fijas

## **2.- CASINO PINAMAR**

### **ESPACIO:**

El adjudicatario, deberá proveer un espacio físico apto para la construcción y/o cesión, y funcionamiento del Casino de Pinamar, el cual deberá contemplar como mínimo de una superficie de mil quinientos (1500) metros cuadrados para uso integral de la sala de juegos y novecientos (900) metros cuadrados, para dependencias internas operativas, administrativas, de descanso, vestuarios, baños, depósitos y laboratorio. El plazo previsto para la finalización de dicha obra, será como máximo de veinticuatro (24) meses.

El casino deberá contemplar, los siguientes requerimientos:

**-Slots:** Cien (100)



**-Mesas:** Diecinueve (19) mesas de Juego de Paño, las que deberán contener:

- \* Doce (12) Mesas de Ruleta Americana
- \* Dos (2) Mesas de Punto y Banca
- \* Dos (2) Mesas de Black Jack
- \* Dos (2) Mesas de Póker
- \* Una (1) Mesa grande de Craps

Paños de juego: Se calcula en base doble por número de mesas a los efectos de tener stock de reposición.

La distribución de las Mesas de Paño será realizada de acuerdo al criterio adoptado por el INSTITUTO.

**SECTOR CASINO:** El espacio cuyo uso se cede, deberá poseer:

**Superficies en distribución:**

- Setecientos (**700 M2**) Metros Cuadrados para Máquinas
- Seiscientos (**600 M2**) Metros Cuadrados para Mesas
- Doscientos (**200 M2**) Metros Cuadrados para restaurantes y afines

**Superficie para áreas del Circuito de Valores:**

- Sector de Cajas de 7m x 4m = **28 M2**
- Ante-tesoro de Fichas con Cajas Internas y Oficina de 6m x 5m = **30 M2**
- Tesoro de Fichas de 3m x 3m = **9 M2**
- Ante-tesoro de Efectivo con Cajas Internas y Oficina de 4m x 5m = **20 M2**
- Tesoro de Efectivo de 3m x 3m = **9 M2**
- Sala de Conteo de Drop de 8m x 5m = **40 M2**



- Pasillos de **1.20 m de ancho**

#### **Superficie de la Sala de Monitores del INSTITUTO**

- Una Sala de Control
- Oficina y Sala de Edición
- Descanso para personal
- Baños Internos
- **Superficie: 6m x 5m = 30 M2**

#### **Superficie de la Sala de Monitores de la Empresa**

Una Sala de Control

Oficina y Sala de Edición

**Superficie: 4 m x 5 m = 20 M2**

#### **Superficie de Áreas Administrativas INSTITUTO y Empresa**

Áreas de Gerencias, Subgerencias, Contabilidad, Cabina, Sistemas, Atención al Cliente, Servicio Médico, Seguridad, Guardarropas, Limpieza, Depósito y Laboratorio = **360 M2**

#### **Superficie de la Sala de Baños (Público y Personal) – Vestuarios y Descanso del personal**

Incluyen personal de la Empresa, del INSTITUTO y para el público, en tres (3) Baterías por separado para masculinos y femeninos. Más área destinada al Descanso de Personal. Oficinas Gremiales

Total: **350 M2**

#### **Contadoras y clasificadoras de billetes:**

- Una (1) Glory UW 500 (4 bolsillos de proceso + 2 de rechazo de los cuales

203



uno es para billetes dudosos y otros para errores mecánicos), o similar de igual o mejor prestación. Equipo que lee TITO.

- Tres (3) Glory GFB 801, o similar de igual o mejor prestación.
- Una (1) Glory GFS 120 (equipo de 2 bolsillos, con tapa anti polvo en el bolsillo de proceso), o similar de igual o mejor prestación.
- Tres (3) Lámparas Detectoras de Billetes Falsos marca Royal ND 140 luz UV + luz blanca, o similar de igual o mejor prestación.
- Una (1) Enfajadora G&D BB 40 (solo para uso continuo heavy duty), o similar de igual o mejor prestación.

#### Cámaras CCTV:

El casino deberá contemplar, como mínimo:

- Dieciocho (18) Domos
- Cuarenta y dos (42) Cámaras Fijas

#### Control de acceso

1 Acceso Personal: Instalación de 1 molinete metálicos de 3 aspas contando con 1 lectores biométricos/tarjetas RFID de entrada y 1 de salida (total 2 lectores)

1 Acceso Proveedores: 1 o 2 lectores biométricos/tarjetas RFID

1 lector de BackUp

20 lectores biométricos/tarjetas RFID para control zonas restringidas internas al edificio

100 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente



### **3.- CASINO TIGRE**

#### **ESPACIO**

El adjudicatario, deberá proveer un espacio físico apto para la construcción y/o cesión, y funcionamiento del Casino de Tigre, el cual deberá contemplar como mínimo una superficie de ocho mil trescientos (8.300) metros cuadrados para uso integral de la sala de juegos y gastronomía y cuatro mil novecientos (4.900) metros cuadrados para dependencias internas operativas, administrativas, de descanso, vestuarios, baños, depósitos y laboratorio. El plazo previsto para la finalización de dicha obra, será como máximo de treinta (30) meses.

El casino deberá contemplar, los siguientes requerimientos:

**-Slots:** Mil quinientos noventa y dos (1592)

**-Mesas:** Setenta y ocho (78) mesas de Juegos de Paño, las que deberán contener:

Veinticuatro (24) Mesas de Ruleta Americana

Dos (2) Mesas de Ruleta Francesa

Catorce (14) Mesas de Punto y Banca

Cuatro (4) Mesas de Mini Baccarat

Catorce (14) Mesas de Black Jack

Catorce (14) Mesas de Poker

Dos (2) Mesas de Poker Central Tres

Dos (2) Mesas de Poker Contra la banca

Craps (2) Mesas grande de Craps



Paños de juego: Se calcula en base doble por número de mesas a los efectos de tener stock de reposición.

La distribución de las Mesas de Paño será realizada de acuerdo al criterio adoptado por el INSTITUTO.

**SECTOR CASINO:** El espacio cuyo uso se cede, deberá poseer:

**Superficies en distribución:**

- Seis mil doscientos (**6200 M2**) Metros Cuadrados para Máquinas
- Mil cien (**1100 M2**) Metros Cuadrados para Mesas
- Mil (**1000 M2**) Metros Cuadrados para restaurantes y afines

**Superficie para áreas del Circuito de Valores:**

- Cuatrocientos treinta (**430 M2**) metros cuadrados en total. Para sectores de cajas, tesoro de fichas, tesoro de efectivo, control de valores, tesorería.

**Superficie de la Sala de Monitores del INSTITUTO**

- Una Sala de Control
- Oficina y Sala de Edición
- Descanso para personal
- Baños Internos
- **Superficie: 6m x 5m = 30 M2**

**Superficie de la Sala de Monitores de la Empresa**

Una Sala de Control

Oficina y Sala de Edición

**Superficie: 4 m x 5 m = 20 M2**



### **Superficie de Áreas Administrativas INSTITUTO y Empresa**

Áreas de Gerencias, Subgerencias, Contabilidad, Cabina, Sistemas, Atención al Cliente, Servicio Médico, Seguridad, Guardarropas, Limpieza, Depósito y Laboratorio = **3460 M2**

### **Superficie de la Sala de Baños (Público y Personal) – Vestuarios y Descanso del personal**

Incluyen personal de la Empresa, del INSTITUTO y para el público, en tres (3) Baterías por separado para masculinos y femeninos. Más área destinada al Descanso de Personal. Oficinas Gremiales

Total: **960 M2**

### **Contadoras y clasificadoras de billetes:**

- Tres (3) Glory UW 600 (8 bolsillos de proceso + 2 de rechazo de los cuales uno es para billetes dudosos y otros para errores mecánicos), o similar de igual o mejor prestación. Equipo que lee TITO.
- Veinticuatro (24) Glory GFB 801, o similar de igual o mejor prestación.
- Diez (10) Glory GFS 120, o similar de igual o mejor prestación.
- Veinticuatro (24) Lámparas Detectoras de Billetes Falsos marca Royal ND 140 luz UV + luz blanca, o similar de igual o mejor prestación.
- Tres (3) Enfajadora G&D BB 40 (solo para uso continuo heavy duty), o similar de igual o mejor prestación.

### **Distribución de cámaras**

El casino deberá contemplar, como mínimo:



## SALA DE JUEGO

- Veinticuatro (24) Mesas de Ruleta Americana; 24 cámaras fijas, más 12 domos
- Dos (2) Mesas de Ruleta Francesa: 2 cámaras fijas, más 1 domo
- Catorce (14) Mesas de Punto y Banca : 14 cámaras Fijas: más 7 domos
- Cuatro (4) Mesas de Mini Baccarat: 4 cámaras fijas, más 2 domos.
- Catorce (14) Mesas de Black Jack: 14 cámaras fijas, más 7 fijas
- Catorce (14) Mesas de Poker: 14 cámaras fijas, más 7 domos
- Dos (2) Mesas de Poker Central Tres: 2 cámaras fijas, más 1 domo
- Dos (2) Mesas de Poker Contra la banca: 2 cámaras fijas, más 1 domo
- Craps (2) Mesas grande de Craps: 4 cámaras fijas, más 2 domo.

Total Cámaras Juego: **120**

## CAJAS

Una (1) Cámara Fija por Caja y un (1) Domo por sector de Cajas en el interior. En el exterior de las Cajas, un (1) Domo y una (1) Cámara Fija por sector de Cajas.

- Nivel 1: 3 Cajas. 3 Cámaras fijas, más 1 domo interno. En el exterior 1 Fija más 1 domo.
- Sala Vip: 1 cámara fija más 1 panorámica interna, más 1 externa fija más 1 domo.
- Nivel 2: 3 Cajas. 3 Cámaras fijas, más 1 domo interno. En el exterior 1 Fija más 1 domo.



- Nivel 3: 5 Cajas (Pago Fichas/Castito). 5 Cámaras fijas, más 1 domo interno. En el exterior 1 Fija más 1 domo.
- 5 Cajas (Venta Fichas / Dólar / TTR). 5 Cámaras fijas, más 1 domo interno. En el exterior 1 Fija más 1 domo.
- 2 cajas Sala especial: 2 cámaras fija, más 1 domo interno. En el exterior 1 Fija más 1 domo.

Total cámaras caja: **37**

### **Cámaras de Máquinas y Áreas Técnicas:**

#### **Nivel 3:**

- Maquinas: 8 Domos.
- Sala Fumadores: 4 domos.
- Conversión: 3 Fijas más 2 Domos. Núcleo: 3 Fijas.
- Pasillo Técnico: 7 Fijas
- Tesoro de Efectivo: 1 Fija
- Tesoros de Cilindro: 2 Fijas. Una interna y un externa
- Comedor: 2 Fijas más 1 Domo
- Administración: 4 Fijas y 3 Domo
- Seguridad: 1 Fija
- Descanso Personal: 5 Fijas



Total Nivel 3: **46**

**Nivel 2:**

- Maquinas: 22 Domos
- Sala Fumadores: 7 domos
- Caja Central: 3 Fijas más 2 domos
- Naipes: 2 Fijas
- Of Juego: 1 Fija

Total Nivel 2: **37**

**Nivel 1:**

Entrada: 2 Fijas

Maquinas: 21 Domos.

Sala Vip: 5 Domos.

Tesorería Operativa: 8 Domos 5 Cámaras Fijas

Ingresos / Enfermería: 6 Fijas

Total Nivel 1: **47**

Total CAMARAS DE MAQUINAS más AREAS TECNICAS: **130**

Exterior: 5 Domos

**Total Cámaras: 292**

En caso de poder ubicar alternadamente mesas de paño en otros niveles, se necesitaran otras 20 cámaras adicionales.

**Máximo de Cámaras: 312****Control de Acceso:**

1 Entrada de Personal: Instalación de 2 molinetes metálicos de 3 aspas contando con 2 lectores biométricos/tarjetas RFID de entrada y 2 de salida (total 4 lectores)

1 Entrada Proveedores: 1 o 2 lectores biométricos/tarjetas RFID

2 lectores BackUp

20 lectores biométricos/tarjetas RDIF para control zonas restringidas internas al edificio

200 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente

**4.- CASINO MIRAMAR:****ESPACIO**

El adjudicatario, deberá proveer un espacio físico apto para la construcción y/o cesión, y funcionamiento del Casino de Miramar, el cual deberá contemplar como mínimo una superficie de un mil trescientos diez (1310) metros cuadrados para uso integral de la sala de juegos, y quinientos veinticinco (525) metros cuadrados para dependencias internas operativas, administrativas, de descanso, vestuarios, baños, depósitos y laboratorio. El plazo previsto para la finalización de dicha obra, será como máximo de veinticuatro (24) meses.



El casino deberá contemplar, los siguientes requerimientos:

**-Slots:** Doscientos diez (210)

**-Mesas:** Dieciocho (18) Mesas de Juego de Paño, las que deberán contener:

\* Doce (12) Mesas de Ruleta Americana

\* Dos (2) Mesas de Punto y Banca

\* Dos (2) Mesas de Black Jack

\* Dos (2) Mesas de Poker

Paños de juego: Se calcula en base doble por número de mesas a los efectos de tener stock de reposición.

La distribución de las Mesas de Paño será realizada de acuerdo al criterio adoptado por el INSTITUTO.

**SECTOR CASINO:** El espacio cuyo uso se cede, deberá poseer:

**Superficies en distribución:**

- Cuatrocientos (**400 M2**) Metros Cuadrados para Máquinas
- Trescientos diez (**310 M2**) Metros Cuadrados para Mesas
- Seiscientos (**600 M2**) Metros Cuadrados para restaurantes y afines

**Superficie para áreas del Circuito de Valores:**

- Sector de Cajas de 7m x 4m = **28 M2**
- Ante-tesoro de Fichas con Cajas Internas y Oficina de 6m x 5m = **30 M2**
- Tesoro de Fichas de 3m x 3m = **9 M2**
- Ante-tesoro de Efectivo con Cajas Internas y Oficina de 4m x 5m = **20 M2**
- Tesoro de Efectivo de 3m x 3m = **9 M2**



- Sala de Conteo de Drop de 8m x 5m = **40 M2**
- Pasillos de **1.20 m de ancho**

#### **Superficie de la Sala de Monitores del INSTITUTO**

- Una Sala de Control
- Oficina y Sala de Edición
- Descanso para personal
- Baños Internos
- **Superficie: 6m x 5m = 30 M2**

#### **Superficie de la Sala de Monitores de la Empresa**

Una Sala de Control

Oficina y Sala de Edición

**Superficie: 4 m x 5 m = 20 M2**

#### **Superficie de Áreas Administrativas INSTITUTO y Empresa**

Áreas de Gerencias, Subgerencias, Contabilidad, Cabina, Sistemas, Atención al Cliente, Servicio Médico, Seguridad, Guardarropas, Limpieza, Depósito y Laboratorio = **360 M2**

#### **Superficie de la Sala de Baños (Público y Personal) – Vestuarios y Descanso del personal**

Incluyen personal de la Empresa, del INSTITUTO y para el público, en tres (3) Baterías por separado para masculinos y femeninos. Más área destinada al Descanso de Personal. Oficinas Gremiales

Total: **350 M2**

Contadoras y clasificadoras de billetes:



- Dos (2) Glory UW 500 (4 bolsillos de proceso + 2 de rechazo de los cuales uno es para billetes dudosos y otros para errores mecánicos), o similar de igual o mejor prestación. Equipo que lee TITO.
- Seis (6) Glory GFB 801, o similar de igual o mejor prestación.
- Dos (2) Glory GFS 120 (equipo de 2 bolsillos, con tapa anti polvo en el bolsillo de proceso), o similar de igual o mejor prestación.
- Tres (3) Lámparas Detectoras de Billetes Falsos marca Royal ND 140 luz UV + luz blanca, o similar de igual o mejor prestación.
- Una (1) Enfajadora G&D BB 40 (solo para uso continuo heavy duty), o similar de igual o mejor prestación.

#### Cámaras CCTV:

El casino deberá contemplar, como mínimo:

- Veinte (20) Domos
- Cincuenta y tres (53) Cámaras Fijas

#### Control de acceso

1 Acceso Personal: Instalación de 1 molinete metálicos de 3 aspas contando con 1 lectores biométricos/tarjetas RFID de entrada y 1 de salida (total 2 lectores)

1 Acceso Proveedores: 1 o 2 lectores biométricos/tarjetas RFID

1 lector de BackUp

20 lectores biométricos/tarjetas RFID para control zonas restringidas internas al edificio

100 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente



## **5.- CASINO MONTE HERMOSO**

### **ESPACIO:**

El adjudicatario, deberá proveer un espacio físico apto para la construcción y/o cesión, y funcionamiento del Casino de Monte Hermoso, el cual deberá contemplar como mínimo una superficie de un mil quinientos (1500) metros cuadrados para uso integral de la sala de juegos, y novecientos (900) metros cuadrados para dependencias internas operativas, administrativas, de descanso, vestuarios, baños, depósitos y laboratorio. El plazo previsto para la finalización de la obra, será como máximo de veinticuatro (24) meses.

El casino deberá contemplar, los siguientes requerimientos:

**-Slot:** Noventa (90)

**-Mesas:** Diecinueve (19) Mesas de Juegos de Paño, las que deberán contener:

- Doce (12) Mesas de Ruleta Americana
- Dos (2) Mesas de Punto y Banca
- Tres (3) Mesas de Black Jack
- Dos (2) Mesas de Poker Cash Game

Paños de juego: Se calcula en base doble por número de mesas a los efectos de tener stock de reposición.

**SECTOR CASINO:** El espacio cuyo uso se cede, deberá poseer:

### **Superficies en distribución:**

- Setecientos (**700 M2**) Metros Cuadrados para Máquinas
- Seiscientos (**600 M2**) Metros Cuadrados para Mesas
- Doscientos (**200 M2**) Metros Cuadrados para restaurantes y afines



### **Superficie para áreas del Circuito de Valores:**

- Sector de Cajas de 7m x 4m = **28 M2**
- Ante-tesoro de Fichas con Cajas Internas y Oficina de 6m x 5m = **30 M2**
- Tesoro de Fichas de 3m x 3m = **9 M2**
- Ante-tesoro de Efectivo con Cajas Internas y Oficina de 4m x 5m = **20 M2**
- Tesoro de Efectivo de 3m x 3m = **9 M2**
- Sala de Conteo de Drop de 8m x 5m = **40 M2**
- Pasillos de **1.20 m de ancho**

### **Superficie de la Sala de Monitores del INSTITUTO**

- Una Sala de Control
- Oficina y Sala de Edición
- Descanso para personal
- Baños Internos
- **Superficie: 6m x 5m = 30 M2**

### **Superficie de la Sala de Monitores de la Empresa**

Una Sala de Control

Oficina y Sala de Edición

**Superficie: 4 m x 5 m = 20 M2**

### **Superficie de Áreas Administrativas INSTITUTO y Empresa**

Áreas de Gerencias, Subgerencias, Contabilidad, Cabina, Sistemas, Atención al Cliente, Servicio Médico, Seguridad, Guardarropas, Limpieza, Depósito y Laboratorio = **360 M2**

### **Superficie de la Sala de Baños (Público y Personal) – Vestuarios y Descanso del personal**



Incluyen personal de la Empresa, del INSTITUTO y para el público, en tres (3) Baterías por separado para masculinos y femeninos. Más área destinada al Descanso de Personal. Oficinas Gremiales

Total: **350 M2**

#### Contadoras y clasificadoras de billetes:

- Un (1) Glory UW 500 (4 bolsillos de proceso + 2 de rechazo de los cuales uno es para billetes dudosos y otros para errores mecánicos), o similar de igual o mejor prestación. Equipo que lee TITO.
- Tres (3) Glory GFB 801, o similar de igual o mejor prestación.
- Un (1) Glory GFS 120 (equipo de 2 bolsillos, con tapa anti polvo en el bolsillo de proceso), o similar de igual o mejor prestación.
- Tres (3) lámparas detectoras marca Royal ND 140 luz UV + luz blanca, o similar de igual o mejor prestación.
- Un (1) enfajadora G&D BB 40 (solo para uso continuo heavy duty), o similar.

#### Cámaras CCTV:

El casino deberá contemplar, como mínimo:

- Veintidos (22) Domos
- Cuarenta y dos (42) Cámaras Fijas

#### Control de acceso

1 Acceso Personal: Instalación de 1 molinete metálicos de 3 aspas contando con 1 lectores biométricos/tarjetas RFID de entrada y 1 de salida (total 2 lectores)



1 Acceso Proveedores: 1 o 2 lectores biométricos/tarjetas RFID

1 lector de BackUp

20 lectores biométricos/tarjetas RFID para control zonas restringidas internas al edificio

100 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente

## **ARTÍCULO 19º.- CASINOS A REFACCIONARSE**

### **1.- CASINO ANEXO III DE MAR DEL PLATA (HOTEL HERMITAGE)**

Esta superficie deberá permitir la instalación y funcionamiento de doscientas setenta y seis (276) Máquinas Electrónicas de Juegos de Azar y doce (12) Mesas de juegos de Paño.

El espacio referido deberá ser entregado en condiciones aptas para su uso, con el mobiliario y decoración necesaria para el funcionamiento de una sala de estas características.

**OBRA:** El plazo previsto para la finalización de la obra tendiente a la refacción del presente Casino, será como máximo de ocho (8) meses.

- **Alfombras:** Reemplazo total de la alfombra que cubre la totalidad de las salas de juego,
- **Baños:** (Baños de Publico de Salas de Juego, masculinos y femeninos en “sector de máquinas y sector mesas de paños”; baños de Sala de Descanso de Empleados “masculinos y femeninos”, Baños Sector Oficinas Operativas), remodelación total, incluyendo, cambio de instalaciones, cambio de revestimientos de pisos y paredes, cambio de mesadas, sanitarios y griferías, realización de cielos rasos, iluminación, divisores de box, vidrios, ventilación y espejos.



- **Techos generales:** Trabajos de yeso, pintura, y realización de cielos rasos, de alturas y decoración variables; la altura de los cielorrasos no inferior a cuatro (4.000) metros, sin interferencias y/o sobre techos intermedios que obstaculicen la correcta visión. La posición de las cámaras fijas o móviles y las luminarias es elemental para una adecuada prestación.
- **Losa Externa:** acondicionamiento e impermeabilización de la Losa y Terrazas donde se encuentra el Helipuerto del Hotel Hermitage, en virtud que por debajo del mismo (el subsuelo) se encuentra toda la superficie que abarca las instalaciones del Casino en su totalidad y Cochera de Automóviles y Motos, como así también acondicionamiento y recambio de la totalidad de los desagües y canaletado de pluviales del mencionado lugar.
- **Iluminación:** realización de proyecto de diseño, cambio de artefactos, lámparas en todos los salones, cajas en general, barras y espacios comunes. La iluminación requerida en Sala de Juegos "NO inferior trescientos (300) Lux. Las luminarias para las Mesas y Cajas deberán permitir graduar su intensidad y potencia para evitar reflejos.
- **Cafetería Sala de Juegos:** realización de nuevas barras en Sala de Juegos, fondos de barras y decoración de acuerdo al proyecto integral.
- **Decoración total:** incorporar elementos que mejoren las escalas del espacio en las mesas de juegos y áreas de máquinas, trabajos de pintura, revestimientos de pisos, paredes y columnas, incluir vidrios, espejos y demás complementos como pantallas de Led, y artefactos de iluminación.
- **Espacios de Áreas de Gestión y Operativas:** acondicionamiento, redistribución, decoración necesaria y reemplazo del mobiliario de las oficinas operativas, depósitos, y salas varias con la finalidad de mejorar la distribución actual (Gerencia, Sub-Gerencia de Juego, Contabilidad, Tesorería, Área CCTV monitores, Cabina de equipos y tramites, Área Caja de Conversión, Área Venta-Pago, Oficina Jefe Seguridad Interna, Servicio Médico, Puestos fijos internos de Policía y Bomberos, Pasillos internos, Oficinas de la Empresa, Laboratorio de Maquinas, Deposito Material de Juego.



- **Tesoros de Fichas y Efectivo:** Acondicionamiento interno y externo de los dos (2) Tesoros de Fichas y Efectivo con cajas internas.
- **Seguridad Interna:** Instalación de una (1) oficina para procedimientos de Seguridad Interna ubicada en la Sala de Juego (aledañas a salidas de emergencias).
- **Acceso público con movilidad reducida:** acondicionamiento de la pasarela a nivel de acceso principal hasta nivel sala, por medio de plataforma.
- **Fachada principal:** cambio y/o acondicionamiento de marquesina. Cambio de Puertas de Entradas y acondicionamiento de los dos (2) accesos de público y un (1) acceso de Empleados, pintura, iluminación, carpelería.
- **Vestuario del Personal:** (masculinos y femeninos) extensión del espacio y acondicionamiento techo, piso, revestimiento, pintura, iluminación, mobiliario acorde al sector, Equipo de climatización Frio – Calor.
- **Cajas:** remodelación de los módulos de cajas de la Sala de Juegos con su respectivo mobiliario adecuado y reubicación del resto según proyecto
- **Salidas de Emergencias:** Instalar Puertas Especiales y acondicionar las tres (3) Salidas para una correcta evacuación, respetando las Normas establecidas para tal fin.
- **Cochera de Autos (subsuelo):** Acondicionamiento, señalización, separación de espacios e iluminación del Sector de Cocheras para automóviles y motos, asignado para el Casino con destino al público concurrente.
- **Cafetería Sala de Descanso:** cambio de instalaciones, revestimientos, mesadas, griferías y equipamiento de apoyo.
- **Señalética general:** rediseño e instalación de cartelería y señalética acorde al proyecto de remodelación.
- **Cortinados:** cambio de cortinas en todas las aberturas.
- **Guardarropas para el público:** acondicionar como mobiliario específico para el sector.
- **Sector “Centro de Atención al cliente”:** acondicionar con mobiliario específico para el lugar.



- **Sala de Espectáculos:** Decoración total y cambio de mobiliario y accesorios con el agregado del ítem “f”
- **Pintura:** incluir acondicionamiento de paredes y columna
- **Cambio de Sillas:** reemplazo total del parque de sillas de doscientas setenta y seis (276) para Máquinas Electrónicas de Juego de Azar.

### Equipamiento:

Se requerirá como mínimo:

**-Slots:** Doscientas setenta y seis (276).

**-Mesas:** Doce (12) Mesas de Juegos de Paño, las que deberán contener:

- \* Ocho (8) Mesas de Ruleta Americana
- \* Dos (2) Mesas de Punto y Banca
- \* Dos (2) Mesas de Black Jack

Paños de juego: Se calcula en base doble por número de mesas a los efectos de tener stock de reposición.

### Contadoras y clasificadoras de billetes:

- Dos (2) Glory UW 500 (4 bolsillos de proceso + 2 de rechazo de los cuales uno es para billetes dudosos y otros para errores mecánicos), o similar de igual o mejor prestación. Equipo que lee TITO.
- Seis (6) Glory GFB 801, o similar de igual o mejor prestación.
- Dos (2) Glory GFS 120 (equipo de 2 bolsillos, con tapa anti polvo en el bolsillo de proceso), o similar de igual o mejor prestación.



- Tres (3) Lámparas Detectoras de Billetes Falsos marca Royal ND 140 luz UV + luz blanca, o similar de igual o mejor prestación.
- Una (1) Enfajadora G&D BB 40 (solo para uso continuo heavy duty), o similar.

#### Cámaras CCTV:

El casino deberá contemplar, como mínimo:

- Diecinueve (19) Domos
- Cincuenta y tres (53) Cámaras Fijas

#### Control de acceso:

1 Acceso Personal: Instalación de 1 molinete metálicos de 3 aspas contando con 1 lectores biométricos/tarjetas RFID de entrada y 1 de salida (total 2 lectores)

1 Acceso Proveedores: 1 o 2 lectores biométricos/tarjetas RFID

1 lector de BackUp

20 lectores biométricos/tarjetas RFID para control zonas restringidas internas al edificio

100 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente

## **2.- CASINO CENTRAL**



Esta superficie deberá permitir como mínimo la instalación y funcionamiento de ochocientos trece (813) Máquinas Electrónicas de Juegos de Azar y ochenta (80) Mesas de juegos de Paño.

El espacio referido deberá ser entregado en condiciones aptas para su uso, con el mobiliario y decoración necesaria para el funcionamiento de una sala de estas características.

**OBRA:** El plazo previsto para la finalización de la obra tendiente a la refacción del presente Casino, será como máximo de doce (12) meses.

1. **Alfombras:** Reemplazo total de la alfombra que cubre la totalidad de las salas de juego y las escaleras de acceso de las mismas
2. **Baños:** remodelación total, incluyendo, cambio de instalaciones, cambio de revestimientos de pisos y paredes, cambio de mesadas, sanitarios y griferías, realización de cielos rasos, iluminación, divisores de box, vidrios y espejos.
3. **Techos generales:** Trabajos de yeso, pintura, y realización de cielos rasos, de alturas y decoración variables.
4. **Iluminación:** realización de proyecto de diseño, cambio de artefactos, lámparas en todos los salones, boleterías, barras y espacios comunes.
5. **Cafetería:** realización de nuevas barras, fondos de barras y decoración de acuerdo al proyecto integral.
6. **Decoración total:** incorporar elementos que mejoren las escalas del espacio en las mesas de juegos y áreas de máquinas, trabajos de pintura, revestimientos de pisos, paredes y columnas, incluir vidrios, espejos y demás complementos como pantallas de Led, y artefactos de iluminación.
7. **Ascensores:** cambio de cabina y máquina.
8. **Acceso público con movilidad reducida:** realización de una pasarela a nivel de acceso principal hasta nivel sala Rambla, por medio de plataforma.
9. **Fachada principal:** cambio y/o acondicionamiento de marquesina y persianas, puesta en valor de las farolas de la puerta principal de acceso.



Acondicionamiento de acceso sobre la calle Rivadavia de solado, cielo raso, iluminación, y cartelería.

10. **Puerta de acceso:** puesta en valor de puertas de bronce en acceso principal y cambio de carpintería en acceso de calle Rivadavia y sala Rambla.
11. **Cajas:** remodelación de las cajas de Hall Central, y reubicación del resto según proyecto
12. **Ventanas:** cambio de aberturas existentes por aberturas pvc.
13. **Terrazas:** acondicionamiento del solado original, iluminación, climatización y mobiliario.
14. **Cocina central:** cambio de instalaciones, revestimientos, mesadas, griferías y equipamiento de apoyo.
15. **Impermeabilización:** realización de trabajos de impermeabilización en cubierta y sectores afectados.

#### **Equipamiento:**

Se requerirá como mínimo:

**-Slot:** Ochocientos trece (813)

**-Mesas:** Ochenta (80) Mesas de Juegos de Paño, las que deberán contener:

- Cuarenta y ocho (48) Mesas de Ruleta Americana
- Ocho (8) Mesas de Ruleta Francesa
- Doce (12) Mesas de Punto y Banca
- Dieciséis (16) Mesas de Black Jack
- Ocho (8) de Poker Texas Holdem
- Dos (2) Mesa grande de Craps

Paños de juego: Se calcula en base doble por número de mesas a los efectos de tener stock de reposición.



#### Contadoras y clasificadoras de billetes:

- Dos (2) Glory UW 600 (8 bolsillos de proceso + 2 de rechazo de los cuales uno es para billetes dudosos y otros para errores mecánicos), o similar de igual o mejor prestación. Equipo que lee TITO.
- Treinta y un (31) Glory GFB 801, o similar de igual o mejor prestación.
- Cuatro (4) Glory GFS 120 (equipo de 2 bolsillos, con tapa anti polvo en el bolsillo de proceso), o similar de igual o mejor prestación.
- Nueve (9) lámparas detectoras marca Royal ND 140 luz UV + luz blanca, o similar de igual o mejor prestación.
- Dos (2) enfajadoras G&D BB 40 (solo para uso continuo heavy duty), o similar de igual o mejor prestación.

#### Expendio de tabaco y creación de club de fumadores

- **Bristol (Sector Rivadavia):** acondicionamiento del sector denominado Bristol de acorde al proyecto, para generar el nuevo salón de fumador.
- **Instalación eléctrica y cableado estructurado:** realización a nuevo toda la instalación eléctrica y de cableado estructurado con sus correspondientes certificaciones.
- **Decoración total:** incorporar elementos que mejoren la imagen del área, trabajo de pintura, revestimientos de pisos, paredes y columnas, e incluir vidrios, espejos y demás complementos como pantallas de Led, y artefactos de iluminación.
- **Techos generales:** Trabajos de yeso, pintura, y realización de cielos rasos, de alturas y decoración variables.
- **Cafetería:** creación de un nuevo sector para una nueva cafetería, fondos de barras y decoración de acuerdo al proyecto.



- **Puertas acceso salón fumador:** Se deberá realizar una exclusiva por medio de puertas de blindex automatizadas para la separación de áreas, fumadores / no fumadores.

#### **Sala Rambla**

- **Decoración total:** incorporar elementos que mejoren la imagen del área, trabajo de pintura, revestimientos de pisos, paredes y columnas, e incluir vidrios, espejos y demás complementos como pantallas de Led, y artefactos de iluminación.
- **Pintura:** incluir acondicionamiento de paredes y columnas
- **Techos generales:** Trabajos de yeso, pintura, y realización de cielos rasos, de alturas y decoración variables.
- **Puertas de acceso:** cambio de puertas existentes.

#### **Equipamiento**

- **Mobiliario cafeterías:** reemplazo de mesas, sillas y muebles acorde al proyecto.
- **Señalética general:** rediseño e instalación de cartelera y señalética acorde al proyecto.
- **Cortinados:** cambio de cortinas en todas las aberturas.
- **CCTV y Equipamiento sala de Monitoreo:** Actualización del sistema de seguridad y adecuación y actualización del equipamiento que comprenderá:

Se requiere también para esta contratación el arreglo integral con materiales de repuesto y la reinstalación del siguiente equipamiento existente:

- Sesenta y dos (62) Cámaras fijas analógicas.
- Doce (12) Cámaras domo analógico American Dynamics modelo Optima.
- Siete (7) DVR's Intellex.



El equipamiento mencionado, debe ser reinstalado e integrado al nuevo sistema VMS de forma tal que el operador pueda operar desde su puesto de operación tanto las cámaras nuevas con tecnología IP como así también las analógicas reinstaladas.

Tanto las sesenta y dos (62) cámaras analógicas como los doce (12) domos analógicos deben grabarse dentro de los 7 DVR'S. Se solicitará también el reemplazo de los discos de los 7 DVR's por discos diseñados para peración 24x7 llevando a los 7 equipos DVR a la máxima capacidad de disco soportada.

Para el movimiento de las cámaras domo analógicas se debe contemplar la reinstalación de los traductores de código existentes o el agregado de equipamiento nuevo que simplifique el control del movimiento de dichas cámaras. El control de los domos analógicos se debe realizar desde la misma consola desde la cual se mueven los domos IP.

El cableado de las cámaras y los domos analógicos que se reinstalen debe ser nuevo, utilizando para ello cables del tipo:

Para el video:RG-59/U (de cobre con una cobertura del 98%)

Para datos RS-422: Belden 9729.

Para Datos Sensornet: Belden 8442.

Para Datos Manchester: Belden 8760.

Detalle de ubicación geográfica de las cámaras a instalar.

Ubicación de las Cámaras del Sistema IP a adquirirse.

### **Entrepiso**

Cámaras Fijas: Sin Cámaras IP



Domos: Sin Cámaras IP

### **Primer Piso**

#### **Cámaras Fijas**

Sala de Juego Vivo: 01 a 72 – 95 a 98 – 106 a 111

Sala de Máquinas: 99 a 105 – 112 a 120

Sectores de Cajas: 73 a 82 – 87 a 91 – 83 a 86 – 92 y 93

Tesoros: 132 a 135 – 123 a 127

Sectores de Acceso: 121 y 122 – 128 a 131 – 136

#### **Domos:**

Sala de Juego Vivo: 01 a 46 – 81 y 82

Sala de Máquinas: 47 a 52 – 54 y 55 – 74 a 78

Sectores de Cajas: 66

Tesoros: 83 a 87 – 60 – 62 a 65 – 67 y 68

Sectores de Acceso: 56 a 59 – 61 – 69 a 73

Salas N° 1 y N° 3: 79 y 80

### **Planta Baja**

#### **Cámaras Fijas**

Sala de Slots: 137 a 142

Sector de Cajas: 94



Externas: 01 a 08

### **Domos**

Sala de Slots: 88 a 93

Sector de Acceso: 53 y 94

Externos: 01 a 06

### **Subsuelo**

Cámaras Fijas: Sin Cámaras IP

Domos: Sin Cámaras IP

**Total cámaras: 250**

Ubicación de las Cámaras del Sistema Analógico existente.

### **Entrepiso**

#### **Cámaras Fijas**

Sala de Monitores: 46 a 50

Acceso Departamento Personal: 61 y 62

#### **Domos**

Sin domos existentes



## Primer Piso y Planta Baja

### Cámaras Fijas

Sala N° 1:	01 y 02
Sala N° 3:	03 y 04
Acceso Sala Rambla:	35 y 37
Acceso Principal de Público:	44 y 45
Confitería Sala:	07 y 08
Salida Puerta N° 4:	09 a 11 – 38 a 43
Resto Bar:	12 a 15
Salida Puerta N° 1, N° 2 y N° 3:	05 y 06 – 16 a 28
Pasillos Internos:	29 a 33
Sala de Descanso:	34 y 36

### Domos

Hall Central:	01 y 02
Acceso Sala Rambla:	10
Salida Puerta N° 2:	07
Resto Bar:	03 a 06
Sala de Descanso:	08 y 09

### Subsuelo

### Cámaras Fijas



Sala de Máquinas: 52 a 59

Estación de EDEA: 60

Salida a Playa: 51

### **Domos**

Sala de Máquinas: 11 y 12

**Total cámaras: 74**

- **Control de acceso:**

Puerta 1 Acceso Personal: Instalación de 4 molinetes metálicos de 3 aspas contando con 4 lectores biométricos/tarjetas RFID de entrada y 4 de salida (total 8 lectores)

Puerta 4 Acceso Personal: Instalación de 3 molinetes metálicos de 3 aspas contando con 3 lectores biométricos/tarjetas RFID de entrada y 3 de salida (total 6 lectores)

2 Pilares Barra para proveedores e invitados con un lector biométricos/tarjetas RFID por pilar

2 lectores de BackUp

20 lectores biométricos/tarjetas RFID para control zonas restringidas internas al edificio

15 Cerradura magnética de 600 lb

2 Pestillo Eléctrico

2 Puertas de control de proveedores, bicicletas y anti-pánico

11 Brazos Cierra Puerta Hidráulico



200 Tarjetas de proximidad RFID ICLASS/Mifare o equivalente



## **ANEXO I**

### **ACUERDO DE CONFIDENCIALIDAD**

Entre el Instituto Provincial de Lotería y Casinos, en adelante el INSTITUTO con domicilio en calle 46 N° 581 de la ciudad de La Plata, representada en este acto por su presidente ..... y por la otra, ....., representada por, ....., con domicilio en ..... en adelante “ LA ADJUDICATARIA”



convienen en celebrar el presente ACUERDO DE CONFIDENCIALIDAD de acuerdo a las prescripciones que a continuación se expresan:

PRIMERO: Toda información, datos, ideas, conceptos, Know-How y, técnicas que proporcione el INSTITUTO a “LA ADJUDICATARIA” para la prestación del servicio contratado será considerada información confidencial.

SEGUNDO: “LA ADJUDICATARIA” se compromete a no divulgar, utilizar ni revelar a terceros la información confidencial obtenida con motivo de la presente contratación, ya sea intencionalmente, por falta de cuidado en su manejo, en forma personal o bien a través de sus empleados, agentes y/o subcontratistas, obligándose a hacer un uso responsable de dicha información de igual manera que lo hace con la información propia de carácter confidencial, la cual bajo ninguna circunstancia podrá estar por debajo de los estándares aceptables de debida diligencia y prudencia para este tipo de operaciones.

TERCERO: “LA ADJUDICATARIA” podrá ser relevada de la obligación precedentemente señalada mediante autorización escrita del INSTITUTO.

CUARTO: “LA ADJUDICATARIA” se compromete a entregar al INSTITUTO todo documento o material de cualquier tipo – incluyendo pero no limitando a copias, apuntes, anotaciones, faxes, email, etc. – que contenga la información confidencial y/o las copias que de los mismos se hubiere obtenido durante la ejecución del servicio contratado al cesar las causas por las cuales le fueron entregados o bien cuando el INSTITUTO así lo requiera.



QUINTO: Las obligaciones asumidas en el presente acuerdo se hacen extensivas a los prestadores, contratistas, subcontratistas, empleados, agentes y/o cualquier otra persona vinculada con LA ADJUDICATARIA, respondiendo esta por cualquier incumplimiento por parte de aquellos.

SEXTO: El incumplimiento por parte de LA ADJUDICATARIA, ya sea en forma personal o a través de las personas precedentemente mencionadas, de las obligaciones asumidas en el presente ACUERDO DE CONFIDENCIALIDAD lo hará responsable de los daños y perjuicios que dicho incumplimiento genere o sea capaz de generar al INSTITUTO, sin perjuicio de las acciones que ésta pueda deducir a efectos de lograr el cese de la conducta contraria al mismo.

El presente acuerdo empezará a regir a partir del momento en que el INSTITUTO transmita a LA ADJUDICATARIA por cualquier medio la primer INFORMACION CONFIDENCIAL y su vigencia se mantendrá hasta un año posterior al vencimiento del contrato respectivo o de su rescisión por cualquier motivo.

Las partes fijan como domicilios especiales los arriba indicados, donde se tendrán por válidas todas las notificaciones que se cursaren con relación al presente acuerdo.

Firmado en dos (2) ejemplares, en la ciudad de La Plata, a los .....



## ANEXO II

### PLANILLA DE COTIZACIÓN:

**Renglón 1:** Por la provisión de un servicio integral destinado a los Casinos de Tigre y Pinamar, comprensivo de la provisión y mantenimiento de máquinas electrónicas de juegos de azar automatizadas, el control on line de las mismas, la construcción y/o cesión y puesta en valor de las distintas salas de juego, y una variedad de servicios complementarios y anexos a la actividad lúdica.

PORCENTAJE DE LA RECAUDACION
%

**En letras:**

**Renglón 2:** Por la provisión de un servicio integral destinado a los Casinos de Tandil, Miramar y Anexo III Hotel Hermitage, comprensivo de la provisión y mantenimiento de máquinas electrónicas de juegos de azar automatizadas, el control on line de las mismas, la construcción y/o cesión y puesta en valor de las distintas salas de juego y una variedad de servicios complementarios y anexos a la actividad lúdica.

PORCENTAJE DE LA RECAUDACION
%

**En letras:**



**Renglón 3:** Por la provisión de un servicio integral destinado a los Casinos Central y Monte Hermoso, comprensivo de la provisión y mantenimiento de máquinas electrónicas de juegos de azar automatizadas, el control on line de las mismas, la remodelación, la construcción y/o cesión y puesta en valor de las distintas salas de juego y una variedad de servicios complementarios y anexos a la actividad lúdica.

<b>PORCENTAJE DE LA RECAUDACION</b>
%

**En letras:**



## **ANEXO III**

### **ANEXO – ESPECIFICACIONES TÉCNICAS EQUIPAMIENTO INFORMÁTICO**

#### **INFRAESTRUCTURA Y SALA DE COMPUTOS**

##### **ETDC001 – DATA ROOM**

###### **Descripción general de la obra.**

El siguiente esquema es solo a modo de ejemplo, para describir las oficinas necesarias y el tamaño de las mismas. La obra civil deberá contemplar el desarrollo de:

1.- Data Room: 5 m<sup>2</sup>

Se deberá realizar la adecuación del recinto del nuevo Data Room de acuerdo a los siguientes lineamientos:

- Re-planteo de obra: confección de un diagrama de tareas (GANTT) en conjunto con los responsables de la obra por parte del INSTITUTO.
- Retiro/Desmonte de instalaciones pre-existentes.
- Protección de zonas no afectadas.
- Construcción de un ambiente estanco y seguro para Sala de Servidores: para asegurar la estanqueidad se la sala y un grado de protección ante fuego no inferior a F60: se realizarán los siguientes trabajos sobre paredes perimetrales y cielorraso.



1. Las paredes perimetrales se construirán en Durlock ignífugo.
  2. Piso en cemento revestido en goma o similar.
  3. El cielorraso se montará fijo sobre Durlock ignífugo con estructura de caño estructural para soportar el peso de la estructura resultante.
  4. Se anularán las aberturas existentes, de acuerdo a las reglas del arte.
  5. Se deberá proveer Piso Técnico para este ambiente.
- Instalación de una puerta contra fuego F60, de 1.10 x 2 m, con barral antipático, perno exterior con llave y cierra puerta hidráulico, la misma deberá contar con certificación del INTI y pulsador destraba cerradura; el sentido de apertura será hacia fuera del recinto.
  - Iluminación mediante luminarias 3x36W con plafón fluorescente difusor de acrílico, a fin de asegurar 200lux verticales y 500lux horizontales. El cableado y la canalización de luminarias se realizará a la vista con cañerías tipo Daysa. También se instalará una luz de emergencia.
  - En el caso de oficinas y depósitos:
    1. Las paredes perimetrales y cielorrasos se construirán en Durlock.
    2. Puertas y ventanas en aluminio blanco.
    3. Los Pisos deben ser de materiales incombustibles y resistentes al fuego.
  - Finalizada la obra se deberá entregar una carpeta con la documentación completa de la obra realizada incluyendo manuales de operación e instalación de equipos, procedimientos ante emergencia, planos civiles y unifilares de tableros provistos.

### **Data Room**



Se requiere para esta licitación, la construcción de un nuevo Data Room en el Casino Central el cual deberá incluir los siguientes requerimientos:

- Adquisición de racks para servidores y concentradores de comunicaciones, para permitir un mayor nivel de escalabilidad.
- Hardware y electrónica de red.
- Tabiquería que delimite el área con protección físico-ambiental.
- Instalación de Piso técnico elevado.
- Sistema de climatización de precisión escalable, con control de temperatura y humedad acorde a las necesidades de la sala.
- Instalación de una infraestructura eléctrica acorde por medio de bandejas y salidas por periscopios a flor del piso técnico elevado e instalación de la distribución eléctrica en cada rack.
- Instalación de una infraestructura de datos acorde por medio de bandejas individuales y salidas por periscopios a flor del piso técnico elevado.
- Instalación de patch panel en los racks de comunicaciones y de servidores.
- Instalación de un sistema de detección temprana de incendios.
- Reubicación de la Sala en un espacio de mayores dimensiones, que permita organizar mejor las sub-áreas de trabajo que se desarrollan.

Se deja constancia que las alternativas que planteen los proveedores deberán respetar las siguientes normas y estándares para ambientes de esta naturaleza:

- IRAM –ISO/IEC 27002:2013- Código de Práctica para la Gestión de la Seguridad de la información.
- ISO 27001. Requisitos para los sistemas de gerenciamiento de la Seguridad de la información.



- DDA 669/04 – Política de Seguridad de la Información.
- TIA 942 – Estándar de Infraestructura para Centros de Datos.
- NFPA 75 – Estándar para la protección del equipamiento informático.

### **Racks**

Cantidad: 2 (dos)

1. Rack 19" standard de altura de 42U y profundidad de 1200 mm
2. Puertas delanteras y traseras microperforadas, equipadas con cerradura con llave.
3. Puertas laterales ciegas equipadas con cerradura con llave.
4. PDU x Rack : 2 x Input IEC-320-C20 / output 10 x IEC320-C13 + 2 x IEC-320-C29 / montaje horizontal 1U.

### **KVM Switch**

Cantidad : 1

Conmutador de Teclado monitor y mouse de al menos 4 puertos, capacidad hasta la menos 4 servidores.

### **Monitor LCD Rackeable.**

Cantidad: 1

Monitor LCD 17" Rackrable con Teclado y Mouse incorporado en bodega pligable de 2 U de altura.



## ETDC002 – DATA ROOM

### Descripción general de la obra.

El siguiente esquema es solo a modo de ejemplo, para describir las oficinas necesarias y el tamaño de las mismas. La obra civil deberá contemplar el desarrollo de:

- 1.-Data Room: 3.24m<sup>2</sup>

Se deberá realizar la adecuación del recinto del nuevo Data Room de acuerdo a los siguientes lineamientos:

- 1.- Re-planteo de obra: confección de un diagrama de tareas (GANTT) en conjunto con los responsables de la obra por parte del INSTITUTO.
- 2.- Retiro/Desmonte de instalaciones pre-existentes.
- 3.- Protección de zonas no afectadas.
- 4.- Construcción de un ambiente estanco y seguro para Sala de Servidores: para asegurar la estanqueidad se la sala y un grado de protección ante fuego no inferior a F60: se realizarán los siguientes trabajos sobre paredes perimetrales y cielorraso.

- \* Las paredes perimetrales se construirán en Durlock ignífugo.

- \* Piso en cemento revestido en goma o similar.

- \* El cielorraso se montará fijo sobre Durlock ignífugo con estructura de caño estructural para soportar el peso de la estructura resultante.

- \* Se anularán las aberturas existentes, de acuerdo a las reglas del arte.

- \* Se deberá proveer Piso Técnico para este ambiente.



- 5 Instalación de una puerta contra fuego F60, de 1.10 x 2 m, con barral antipático, perno exterior con llave y cierra puerta hidráulico, la misma deberá contar con certificación del INTI y pulsador destraba cerradura; el sentido de apertura será hacia fuera del recinto.
- 6 Iluminación mediante luminarias 3x36W con plafón fluorescente difusor de acrílico, a fin de asegurar 200lux verticales y 500lux horizontales. El cableado y la canalización de luminarias se realizará a la vista con cañerías tipo Daysa. También se instalará una luz de emergencia.
- 7 En el caso de oficinas y depósitos:
  - a. Las paredes perimetrales y cielorrasos se construirán en Durlock.
  - b. Puertas y ventanas en aluminio blanco.
  - c. Los Pisos deben ser de materiales incombustibles y resistentes al fuego.
- 8 Finalizada la obra se deberá entregar una carpeta con la documentación completa de la obra realizada incluyendo manuales de operación e instalación de equipos, procedimientos ante emergencia, planos civiles y unifilares de tableros provistos.

### **Data Room**

Se requiere para esta licitación, la construcción de un nuevo Data Room en el Casino Central el cual deberá incluir los siguientes requerimientos:

- 1 Adquisición de racks para servidores y concentradores de comunicaciones, para permitir un mayor nivel de escalabilidad.
- 2 Hardware y electrónica de red.
- 3 Tabiquería que delimite el área con protección físico-ambiental.
- 4 Instalación de Piso técnico elevado.
- 5 Sistema de climatización de precisión escalable, con control de temperatura y humedad acorde a las necesidades de la sala.



- 6 Instalación de una infraestructura eléctrica acorde por medio de bandejas y salidas por periscopios a flor del piso técnico elevado e instalación de la distribución eléctrica en cada rack.
- 7 Instalación de una infraestructura de datos acorde por medio de bandejas individuales y salidas por periscopios a flor del piso técnico elevado.
- 8 Instalación de patch panel en los racks de comunicaciones y de servidores.
- 9 Instalación de un sistema de detección temprana de incendios.
- 10 Reubicación de la Sala en un espacio de mayores dimensiones, que permita organizar mejor las sub-áreas de trabajo que se desarrollan.

Se deja constancia que las alternativas que planteen los proveedores deberán respetar las siguientes normas y estándares para ambientes de esta naturaleza:

- IRAM –ISO/IEC 27002:2013- Código de Práctica para la Gestión de la Seguridad de la información.
- ISO 27001. Requisitos para los sistemas de gerenciamiento de la Seguridad de la información.
- DDA 669/04 – Política de Seguridad de la Información.
- TIA 942 – Estándar de Infraestructura para Centros de Datos.
- NFPA 75 – Estándar para la protección del equipamiento informático.

## Racks

Cantidad: 1

- a. Rack 19" standard de altura de 42U y profundidad de 1200 mm
- b. Puertas delanteras y traseras microperforadas, equipadas con cerradura y llave.
- c. Puertas laterales ciegas equipadas con cerradura y llave.
- d. PDU x Rack : 2 x Input IEC-320-C20 / output 10 x IEC320-C13 + 2 x IEC-320-C29 / montaje horizontal 1U.

244



### **KVM Switch**

Cantidad : 1

Conmutador de Teclado monitor y mouse de al menos 4 puertos, capacidad hasta al menos 4 servidores.

### **Monitor LCD Rackeable.**

Cantidad: 1

Monitor LCD 17" Rackable con Teclado y Mouse incorporado en bodega pligable de 2 U de altura.

### **ETCCNINT50 – ENLACE A INTERNET SIMETRICO DEDICADO 50Mbps**

Ítem	Característica
Ancho de banda de UPSTREAM	50 Mbps
Ancho de Banda de DOWNSTREAM	50 Mbps
Tecnología Última Milla	Fibra óptica.

### **TCCNINT10 – ENLACE A INTERNET SIMETRICO DEDICADO 10 Mbps**

Ítem	Característica
Ancho de banda de UPSTREAM	10 Mbps
Ancho de Banda de DOWNSTREAM	10 Mbps
Tecnología Última Milla	Fibra óptica.



### ETCCNINT06 – ENLACE A INTERNET SIMETRICO DEDICADO 6 Mbps

Ítem	Característica
Ancho de banda de UPSTREAM	6 Mbps
Ancho de Banda de DOWNSTREAM	6 Mbps
Tecnología Última Milla	indistinto

### CONECTIVIDAD LAN

### CABLEADO ESTRUCTURADO

#### ETCECC001 – CABLEADO ESTRUCTURADO CAT 6 E TIPO 1

#### Cableado de datos – Cantidad: 170 (ciento setenta) puestos de trabajo

##### CATEGORÍA 6 Aumentada

Se proveerá los cables, conectores, patcheras, bastidores, elementos de sujeción, documentación, Garantía de Producto (20 años) y Aplicaciones del Fabricante y demás elementos y herramientas necesarias para la correcta ejecución de los trabajos.

#### Normas y reglamentaciones



Serán de aplicación en este proyecto las siguientes normas y reglamentos:

- Normas ANSI/EIA/TIA 568 B.2 1
- Norma TIA/EIA 568.B.2 Addendum 10 para Categoría 6 Aumentada.
- ISO 11801 Nueva Clase E Aumentada

El cuanto a voz, la red soportará las aplicaciones y servicios provistos por un sistema de Telefonía IP. El fabricante de la solución, deberá certificar ISO 9001.

#### Descripción de la instalación del Sistema de cableado estructurado

El sistema de cableado estructurado a implementar será el Backbone principal del centro de cómputos.

En la parte superior de cada rack se instalará y cableará totalmente un Patch Panel de 24 ports RJ45, los cuales estarán listos para migrar a Paneles Inteligentes – Patch Panels Categoría 6A I-Patch

En el rack concentrador se instalará 1 Patch Panel de 24/48 ports según la concentración de conexiones en cada caso, por cada rack instalado, que concentrarán los Patch Panels de los demás racks. Serán Patch Panels de 1U de rack completos. Se proveerá además, ordenadores de 2U de rack con tapa desmontable por cada patch panel de 24 ports.



El Centro de Cómputos posee una distribución de dos filas paralelas, en uno de los racks, se dispondrá de 1 rack concentrador de cableado que se destinará para instalar los equipos activos de comunicaciones y las patcheras con el cableado proveniente de cada rack.

El cableado se distribuirá por las bandejas instaladas por encima de los racks.

#### Backbone de comunicación entre los MDF e IDF:

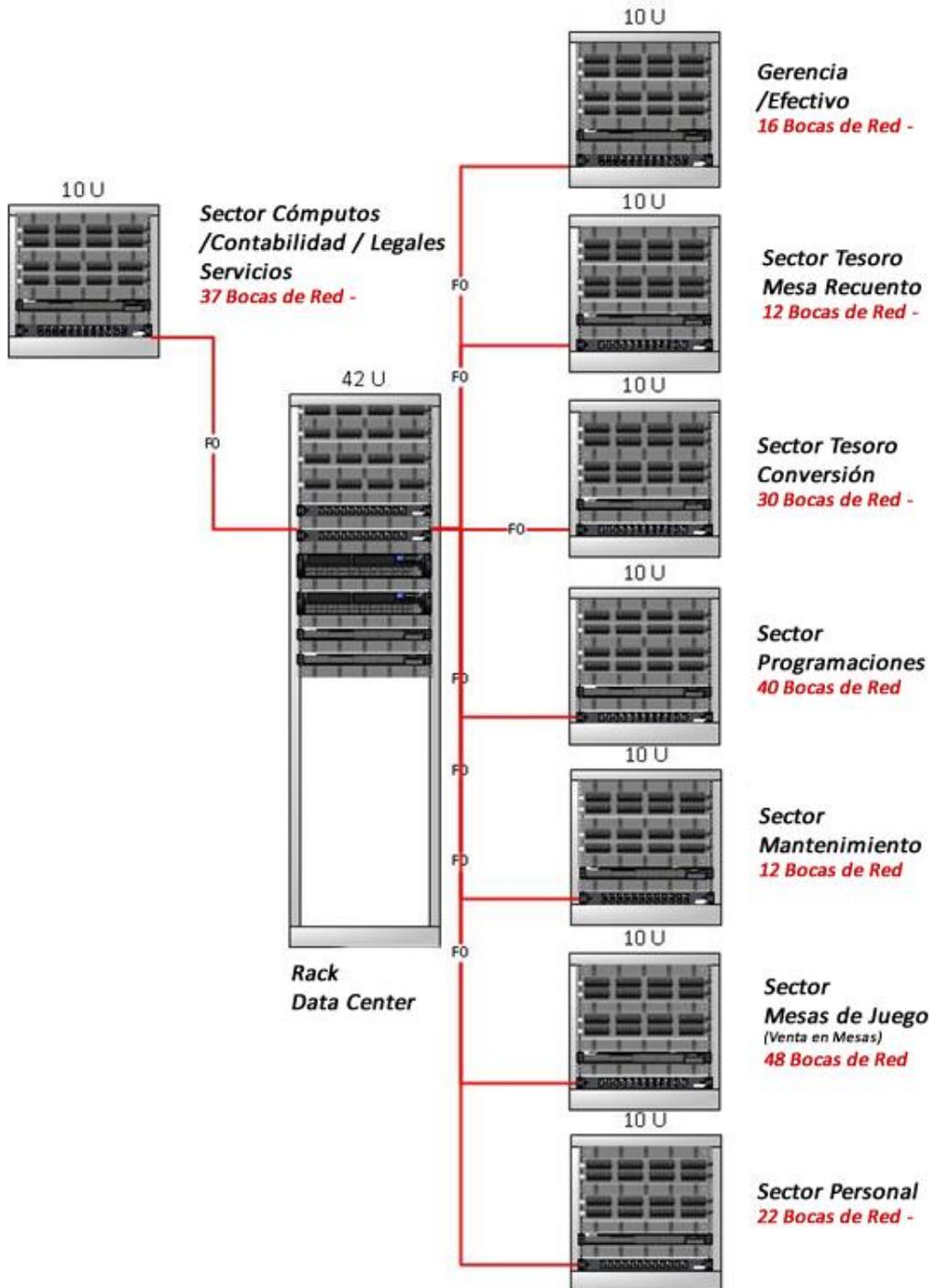
Se dispondrá de dos pares (cuatro pelos) de fibra óptica Multimodo M3 con soporte de 10GB conectada entre los IDF y el MDF. Montados en pachpanel con conectores LC. Se proveerán la cantidad de patchcore de fibra LC a SC de 1 mts necesaria para la interconexión con los switches instalados en los IDF y MDF

#### Cableado de los puestos de trabajo

El sistema de cableado estructurado a implementar para los puestos de trabajo se hará con cable UTP categoría 6. Cada puesto de trabajo deberá ser instalado para datos o voz. En los racks de piso (IDF) se dispondrán de uno o dos pachpanel de 48 bocas en total para datos categoría 6 y uno o dos patchpanel de 48 bocas en total categoría 5e para telefonía con sus respectivos organizadores de cables de 1U para rack con tapa desmontable.



### Esquema de Configuración de Cableado MDF e IDF





### **Garantía y Mantenimiento Preventivo**

Todos los elementos solicitados deberán ser provistos con una garantía escrita por una duración de **3 (tres) años**.

Cualquier elemento que sufra desperfecto y debe ser retirado para su reparación deberá proveerse en su reemplazo uno de similares características hasta que el elemento sea reparado.

Se deberá proveer un mantenimiento preventivo programado del equipamiento solicitado con una frecuencia no mayor a 3 (tres) meses entre visitas.

ETCECC002 - CABLEADO ESTRUCTURADO CAT 6 E TIPO 2

### **ELECTRONICA DE RED**

CONDICIONES PARTICULARES ESPCIFICAS – APLICA A TODOS LOS ITEMS

### **CONDICIONES PARTICULARES ESPECÍFICAS**



- Los equipos ofrecidos deberán ser de igual marca de fábrica siendo la empresa fabricante propietaria de dicha marca, debiendo acreditarse en forma fehaciente tal situación. La marca impresa sobre los equipos debe ser de calidad tal que impida su remoción.

## **B - Respetto de los bienes ofertados**

Los equipos ofertados para los Renglones 1, 2, 3 y 4, deberán ser de la misma marca

Los equipos ofertados para Renglones 5, 6 y 7, deberán ser de la misma marca.

Todas las facilidades, prestaciones, características y especificaciones del hardware y software ofertado que sean necesarias para que dicho hardware y software se ajuste a los requerimientos aquí enunciados, deberán estar disponibles (liberadas al mercado) al momento de la apertura de las Ofertas. No se aceptarán facilidades que sólo estén disponibles en versiones beta de los paquetes de software o a modo de prototipo en el hardware.

1. Todas las facilidades, prestaciones y/o características que se implementen en forma propietaria en los sistemas ofertados, y se encuentren en vías de

estandarización por parte del Proveedor al momento de presentar la propuesta, deberán ser reemplazados, a cargo del Proveedor, si durante el



período de garantía se produce la liberación al mercado del que contenga la implementación del estándar.

2. El bien ofertado deberá estar en producción al momento de la apertura de Ofertas.

Si se dejara de comercializar el bien durante el período entre la presentación de la Oferta y el perfeccionamiento del contrato, la empresa adjudicataria deberá reemplazarlo por el comercializado, el que deberá poseer características técnicas iguales o superiores al ofertado.

La fecha de discontinuidad de soporte tecnológico completo de todos los equipos a proveer deberá ser posterior en, por lo menos, cinco años respecto de la fecha de apertura del presente llamado.

3. El número de serie del equipo deberá ser de calidad tal que imposibilite su remoción y que no pueda ser adulterado, en ambos casos, sin dejar evidencias.
4. Todos los equipos ofertados deberán cumplir con las especificaciones regulatorias de seguridad eléctrica, emisión de radiofrecuencia, emisión electromagnética y emisión de radiación, emitidas por los organismos competentes de los Estados Unidos o Canadá o la Comunidad Europea o Japón.
5. El equipamiento ofrecido deberá cumplir con todas las normas y recomendaciones que hayan emitido los organismos públicos y/o privados,

nacionales e internacionales de competencia. Serán también exigibles las especificaciones que hubiere fijado la Comisión Nacional de Comunicaciones y que se encuentren en vigencia, cumpliendo además las



normas del UIT-T (ex CCITT) de 1988 y conexas, además de los estándares IEEE, y las recomendaciones IETF Request for Comments (RFC) correspondientes.

6. Los bienes ofertados deberán cumplir con las especificaciones técnicas básicas, serán nuevos, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso a que el Comprador será el primer usuario de los equipos desde su fabricación).
7. Todas las funcionalidades solicitadas en las presentes especificaciones técnicas básicas para cada categoría de equipos, deberán operar en forma simultánea sin limitación alguna.

### **C - Respecto a la presentación de Ofertas**

\* La Oferta deberá ser presentada por escrito respetando el orden impuesto en las **“Especificaciones Técnicas Básicas”**, describiendo técnicamente cada uno de los puntos solicitados (leyenda “Especificar”), en forma clara, detallada, precisa y sin ambigüedades. No se admitirá ni se considerará como especificación, descripción o identificación del bien ofrecido leyendas “según pliego” o expresiones de índole similar o referencias a folletos adjuntos

\* Se deberá adjuntar toda la documentación indicada y establecida en estas **“Condiciones Particulares Específicas”** y las **“Especificaciones Técnicas Básicas”**.

\*Se podrá, a los fines de lograr una mejor comprensión de las especificaciones consignadas, incluir folletos técnicos (o información impresa proveniente del sitio oficial de la empresa fabricante) de los equipos,



pudiendo ser presentados en idioma español o en idioma inglés. Se deja establecido que los folletos adjuntos no forman parte de la Oferta

\*Las Especificaciones técnicas básicas presentan, en una matriz, la condición de "Característica y/o Parámetro Requerido", que viene denotada por una letra "R", mientras que la condición de "Característica y/o Parámetro NO Requerido", viene denotada por las letras " NR ".

Aquellos atributos que sean provistos aún cuando no hayan sido requeridos, serán considerados como válidos, no obstante, el cumplimiento en exceso de las condiciones solicitadas, no abundará en beneficio de la Oferta.

#### D - Respecto a la Evaluación de Ofertas

- Evaluación de la documentación presentada
  1. Se evaluará que se haya presentado la documentación requerida en las "**Condiciones Particulares Específicas**" y las "**Especificaciones Técnicas Básicas**". De existir faltantes, la Oferta será declara "**No admisible técnicamente**"

Se verificará la validez y consistencia de dicha documentación.

2. Se verificará que el bien ofrecido cumpla con las "**Condiciones Particulares Específicas**" y las "**Especificaciones Técnicas Básicas**"

. En caso que no cumpla, la Oferta será declarada "**No admisible técnicamente**".



3. El comitente podrá solicitar aclaraciones, a través de notificación fehaciente, donde se establecerá el plazo otorgado para dar respuesta.

### **E - Cursos de Capacitación**

\*El Proveedor, dictará cursos de capacitación relativa a los equipos que provea. El mismo será brindado para hasta un máximo de 2 personas del Organismo Contratante, con conocimientos intermedios y avanzados de networking. Abarcará temas introductorios de networking (sólo a modo de repaso y en la medida de que sea necesario), descripción detallada del equipamiento a nivel técnico funcional, configuración, gestión y administración, management, monitoreo, integración a sistemas de management y monitoreo. Tendrá una duración mínima de 20 (veinte) horas y comprenderá además pruebas prácticas de laboratorio.

\*Los cursos podrán ser dictados en dependencias del Proveedor o en dependencias del Organismo Contratante. En cualquier caso, deberán ser dictados en la Ciudad de La Plata o en la Ciudad Autónoma de Buenos Aires.

El Oferente deberá detallar en su Oferta los cursos incluidos y su temario.

---

### **F - Recepción de bienes**

\*El Adjudicatario deberá proveer para cada equipo, documentación original (no serán aceptadas fotocopias) correspondientes a los bienes entregados, preferentemente en castellano o en su defecto en



inglés, copias en CD-ROM del software componente del sistema y las licencias de uso permanente

## **G - Garantía de los bienes, Soporte y Asistencia**

\* Garantía.

1. Los bienes a suministrar tendrán una garantía de la empresa fabricante por un término mínimo 36 meses, la cual no deberá perderse por la apertura del equipo a efectos de la instalación de alguna interfase o módulo, con autorización del proveedor y/o empresa fabricante.
2. Garantía de buen funcionamiento:
  1. La “Garantía de buen funcionamiento” abarcará todo el período indicado en el Punto 1.1 y deberá cumplir los siguientes requisitos:
    1. La presente garantía incluirá el servicio de reparación por personal calificado con la provisión y el reemplazo de las partes que se encuentren defectuosas por repuestos originales. Los elementos reemplazantes deberán ser de las mismas características o en su defecto equivalentes en su rendimiento según las pautas de calidad establecidas por el fabricante del bien entregado y las exigidas en las “Especificaciones Técnicas Básicas”. Deberá presentarse, en caso de ser requerido, la documentación que respalde lo previamente expuesto



2. A efectos de cumplimentar con el servicio de garantía, el equipamiento se centralizará en una dependencia del organismo contratante dentro de la ciudad de La Plata y su área de influencia incluyendo a la Ciudad Autónoma de Buenos Aires, donde la empresa fabricante deberá repararlo o retirarlo para su reparación. Los gastos de traslado desde y hacia esa dependencia estarán a cargo exclusivo del proveedor. ( Se define al área de influencia de la ciudad de La Plata a los partidos de La Plata, Berisso y Ensenada).
3. La reparación de los bienes deberá ser ejecutada a satisfacción del Comprador. El tiempo transcurrido entre el pedido de reparación y la efectiva reparación de la falla no podrá superar el indicado a continuación para cada categoría de equipos (Renglón). El horario disponible para reclamos deberá ser de 9.00 hs. a 18 hs.
4. Tiempo de reparación:
5. Para equipos del Item 1: 72 hs.
6. Para equipos del Item 2: 72 hs.
7. Para equipos del Item 3: 24 hs.
8. Para equipos del Item 4: 24 hs.
9. Para equipos del Item 5: 12 hs.



10. Para equipos del Item 6: 6 hs.
3. La cantidad de días de indisponibilidad, según se define en las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: **Defectos de Origen - Vicios de Fabricación - Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía** –, no es aplicable en el presente Renglón.
4. Soporte y Asistencia.

Durante el período de garantía establecido en el Punto 1.1, el proveedor brindará soporte y asistencia técnica telefónica, aplicándola a la configuración y problemática que la operatoria habitual de los equipos demande. El horario disponible para consultas será de lunes a viernes de 9.00 a 18.00 hs.

---

ETSEL3CR12PFO - SWITCH CORE L3 12 PUERTO FO}

<b>Conmutador (Switch) de Core Modular y Administrable</b>
<p>Concentrador Switch de Core Modular con las siguientes características:</p> <ul style="list-style-type: none"> <li>• Concentrador Switch para conmutación de tramas LAN.</li> <li>• Deberá contar con servicios de red de capa 2 y 3 (network layer 2 y 3).</li> <li>• Deberá contar con “stack dual” IPv4/IPv6.</li> </ul>



- Deberá incluir los accesorios necesarios para montar en racks estándar de 19”.
- Debe ocupar una altura no superior a <1> unidades de rack.
- Cada unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados en formato papel o mediante medios de almacenamiento digitales.
- Los equipos deberán ser alimentados de 220 V - 50 Hz, monofásico con toma de 3 patas planas, sin necesidad de requerir un transformador adicional.
- Compatibilidad mínima: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet en cobre (IEEE 802.3ab), Gigabit Ethernet en fibra (IEEE 802.3z) y 10 Gigabit Ethernet (IEEE 802.3ae).

#### **CONECTIVIDAD**

- La cantidad de puertos de concentración inicial deberá proveerse mediante la instalación de los módulos correspondientes para los tipos indicados en la tabla que se incluye más abajo.
- En caso de que el acceso a la interfaz física sea implementada mediante transceptores enchufables, los mismos deberán ser del tipo GBIC, mini-GBIC/SFP o similar.
- El chasis ofertado deberá contar con una cantidad de slots libres que le permitan alcanzar la capacidad final indicada en la tabla que se indica más abajo, mediante la simple instalación de los módulos correspondientes.
- Cantidad y tipo de bocas mínimo a incluir en el switch:



Tipo	Cantidad	PoE
SFP 10Gb	12	No

- Todos los puertos deberán soportar IEEE 802.3ad LACP (Link Aggregation Control Protocol) para agrupamiento de enlaces en un único canal de mayor ancho de banda.
- Soporte de Jumbo Frames de al menos 9180 bytes de longitud

#### RENDIMIENTO

- La matriz de conmutación en Layer 2 (switch fabric) deberá contar con una velocidad de conmutación inicial 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.
- La matriz de conmutación en Layer 2 (switch fabric) deberá tener capacidad de escalar, hasta una velocidad de conmutación no inferior a *<68 Gbps>*. Los oferentes deberán explicar técnicamente el modo en que se consigue dicho crecimiento.
- El redireccionamiento en Layer 3 para IPv4 (Layer 3 packet forwarding) será no inferior a *<10 Mpps>* con capacidad de crecer a un mínimo de *<50 Mpps>*.



### **CAPACIDADES DE CAPA 2 (LAYER 2)**

- Soporte de al menos 32000 MAC address de red.
- Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en cualquier puerto según IEEE 802.1 p/Q o por reglas de asignación por port y address MAC.
- Deberá soportar no menos de 1000 VLANs, con posibilidad de escalar a 4000 mediante upgrade de software y/o licencia.
- Soporte de Spanning Tree Protocol según IEEE 802.1D y Rapid Spanning Tree Protocol según IEEE 802.1w.
- Soporte de Multiple Spanning Tree Protocol según IEEE 802.1s para mejorar la eficiencia de convergencia en entornos VLAN.

### **CAPACIDADES DE CAPA 3 (LAYER 3)**

- Soporte de ruteo estático.
- Soporte de "Router Information Protocol", RIPv1, RIPv2.
- Deberá efectuar Routing entre Virtual LANs con protocolos IP (mínimo).
- Deberá ser capaz de rutear OSPF, IS-IS, BGP, PIM, IPv6 mediante upgrade de software y/o licencia.
- Soporte de al menos 24000 rutas unicast en la tabla de ruteo.



### **CALIDAD DE SERVICIO (QoS)**

- Deberá implementar mecanismos para clasificación de tráfico tanto en IPv4 como IPv6.
- Deberá poseer al menos 8 colas de priorización de tráfico por puerto, y al menos una de las colas deberá tener prioridad absoluta en la conmutación de su tráfico por sobre todas las demás, esto es, mientras esta cola tenga tráfico en espera, no podrá procesarse ninguna otra cola.
- Permitirá el manejo de políticas de QoS con criterios asignables sobre layer 2 y 3 (mínimo).
- Deberá soportar IEEE 802.1p/Q para clasificación y priorización de tráfico, IP ToS y DiffServ.
- En cada puerto deberá aceptar la conmutación de tráfico clasificado (TAG) aunque sin rechazar otros tráficos no clasificados (UNTAG), a fin de permitir la conexión de un teléfono IP y una PC en un mismo puerto.
- Deberá poder realizar mapeos 802.1p/Q a DiffServ/ToS y DiffServ/ToS a 802.1p/Q.

### **SEGURIDAD**

- Manejo de Listas de Control de Acceso (ACL) sobre layer 2 a 3 (mínimo).
- Soporte de autenticación IEEE 802.1x
- Soporte de autenticación múltiple (multi-host) IEEE 802.1x
- Deberá ser capaz de realizar autenticación IEEE 802.1x a través de una consulta a un servidor de autenticación del tipo RADIUS acorde a RFC-



2138.

- Soporte de administración encriptada mediante SNMPv3, SSL o SSH.

#### **ADMINISTRACIÓN**

- Agente SNMP según RFC 1157 que permita monitorear el estado y el tráfico del dispositivo en forma remota desde entorno Windows / X Windows. Soporte de MIB II según RFC 1213.
- Se deberán proveer en un medio extraíble todos los bloques de información de management (MIBs) necesarios.
- Capacidad de soportar al menos 4 grupos de RMON.
- Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con las siguientes características:
  1. Capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP según RFC 1350 (cliente y servidor).
  2. El sistema deberá permitir actualizaciones de software en línea sin necesidad de interrumpir su funcionamiento.
  3. Asimismo deberá permitir realizar una copia de resguardo del sistema actual, a fin de tener la capacidad de recuperarlo en caso de que la actualización no funcione adecuadamente.
- Servicio de configuración por medio de consola remota Telnet según RFCs 854/855 sobre transporte TCP/IP según RFCs 793/791.
- Soporte de replicación o copiado de tráfico configurable, ya sea mediante ACL, port, MAC address o VLAN hacia un puerto específico definido por el



administrador para su estudio y análisis.

#### **REDUNDANCIA Y ALTA DISPONIBILIDAD**

- Fuente de alimentación redundante (mínimo 1+1).
- Ventiladores redundantes, reemplazables en caliente.
- Debe poseer la capacidad de stack para datos y permitir tener las fuentes de alimentación dentro del stack trabajando como una fuente común de energía.
- Deberá soportar al menos 8 unidades formando parte de un mismo stack.
- El tráfico dentro del stack debe poseer un bandwidth de como mínimo 450 Gbps.
- Los switches propuestos deberán contar con capacidad de converger una red Wireless y cableada para funcionar como controlador de los puntos de acceso wireless sin el agregado de hardware y mediante licenciamiento opcional.
- El switch propuesto deberá tener la posibilidad de desplegar en un mismo stack, diferentes tecnologías Fibre/Cobre.

ETSWL3CR24PGB



### Conmutador (Switch) de Core Modular y Administrable

Concentrador Switch de Core Modular con las siguientes características:

- Concentrador Switch para conmutación de tramas LAN.
- Deberá contar con servicios de red de capa 2 y 3 (network layer 2 y 3).
- Deberá contar con "stack dual" IPv4/IPv6.
- Deberá incluir los accesorios necesarios para montar en racks estándar de 19".
- Debe ocupar una altura no superior a <1> unidades de rack.
- Cada unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados en formato papel o mediante medios de almacenamiento digitales.
- Los equipos deberán ser alimentados de 220 V - 50 Hz, monofásico con toma de 3 patas planas, sin necesidad de requerir un transformador adicional.
- Compatibilidad mínima: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet en cobre (IEEE 802.3ab), Gigabit Ethernet en fibra (IEEE 802.3z) y 10 Gigabit Ethernet (IEEE 802.3ae).

### CONECTIVIDAD

- La cantidad de puertos de concentración inicial deberá proveerse mediante la instalación de los módulos correspondientes para los tipos indicados en la



tabla que se incluye más abajo.

- En caso de que el acceso a la interfaz física sea implementada mediante transceptores enchufables, los mismos deberán ser del tipo GBIC, mini-GBIC/SFP o similar.
- El chasis ofertado deberá contar con una cantidad de slots libres que le permitan alcanzar la capacidad final indicada en la tabla que se indica más abajo, mediante la simple instalación de los módulos correspondientes.
- Cantidad y tipo de bocas mínimo a incluir en el switch:

Tipo	Cantidad	PoE
10/ 100/ 1000 Base SX	24	No

- Todos los puertos de cobre 10/100/1000BaseT deberán soportar la característica Auto-MDIX, es decir el conector deberá ajustar automáticamente su funcionamiento sin importar si se enchufa un cable directo o uno cruzado.
- Para modo full dúplex los puertos deberán soportar control de flujo mediante IEEE 802.3X.
- Todos los puertos deberán soportar IEEE 802.3ad LACP (Link Aggregation Control Protocol) para agrupamiento de enlaces en un único canal de mayor ancho de banda.
- Soporte de Jumbo Frames de al menos 9180 bytes de longitud



## RENDIMIENTO

- La matriz de conmutación en Layer 2 (switch fabric) deberá contar con una velocidad de conmutación inicial 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.
- La matriz de conmutación en Layer 2 (switch fabric) deberá tener capacidad de escalar, hasta una velocidad de conmutación no inferior a <68 Gbps>. Los oferentes deberán explicar técnicamente el modo en que se consigue dicho crecimiento.
- El redireccionamiento en Layer 3 para IPv4 (Layer 3 packet forwarding) será no inferior a <10 Mpps> con capacidad de crecer a un mínimo de <50 Mpps>.

## CAPACIDADES DE CAPA 2 (LAYER 2)

- Soporte de al menos 32000 MAC address de red.
- Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en cualquier puerto según IEEE 802.1 p/Q o por reglas de asignación por port y address MAC.
- Deberá soportar no menos de 1000 VLANs, con posibilidad de escalar a 4000 mediante upgrade de software y/o licencia.
- Soporte de Spanning Tree Protocol según IEEE 802.1D y Rapid Spanning Tree Protocol según IEEE 802.1w.



- Soporte de Multiple Spanning Tree Protocol según IEEE 802.1s para mejorar la eficiencia de convergencia en entornos VLAN.

### **CAPACIDADES DE CAPA 3 (LAYER 3)**

- Soporte de ruteo estático.
- Soporte de "Router Information Protocol", RIPv1, RIPv2.
- Deberá efectuar Routing entre Virtual LANs con protocolos IP (mínimo).
- Deberá ser capaz de rutear OSPF, IS-IS, BGP, PIM, IPv6 mediante upgrade de software y/o licencia.
- Soporte de al menos 24000 rutas unicast en la tabla de ruteo.

### **CALIDAD DE SERVICIO (QoS)**

- Deberá implementar mecanismos para clasificación de tráfico tanto en IPv4 como IPv6.
- Deberá poseer al menos 8 colas de priorización de tráfico por puerto, y al menos una de las colas deberá tener prioridad absoluta en la conmutación de su tráfico por sobre todas las demás, esto es, mientras esta cola tenga tráfico en espera, no podrá procesarse ninguna otra cola.
- Permitirá el manejo de políticas de QoS con criterios asignables sobre layer 2 y 3 (mínimo).
- Deberá soportar IEEE 802.1p/Q para clasificación y priorización de tráfico, IP ToS y DiffServ.



- En cada puerto deberá aceptar la conmutación de tráfico clasificado (TAG) aunque sin rechazar otros tráficos no clasificados (UNTAG), a fin de permitir la conexión de un teléfono IP y una PC en un mismo puerto.
- Deberá poder realizar mapeos 802.1p/Q a DiffServ/ToS y DiffServ/ToS a 802.1p/Q.

### **SEGURIDAD**

- Manejo de Listas de Control de Acceso (ACL) sobre layer 2 a 3 (mínimo).
- Soporte de autenticación IEEE 802.1x
- Soporte de autenticación múltiple (multi-host) IEEE 802.1x
- Deberá ser capaz de realizar autenticación IEEE 802.1x a través de una consulta a un servidor de autenticación del tipo RADIUS acorde a RFC-2138.
- Soporte de administración encriptada mediante SNMPv3, SSL o SSH.

### **ADMINISTRACIÓN**

- Agente SNMP según RFC 1157 que permita monitorear el estado y el tráfico del dispositivo en forma remota desde entorno Windows / X Windows. Soporte de MIB II según RFC 1213.
- Se deberán proveer en un medio extraíble todos los bloques de información de management (MIBs) necesarios.
- Capacidad de soportar al menos 4 grupos de RMON.



- Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con las siguientes características:
  1. Capacidad de actualización por medio de protocolo FTP según RFC 959 ó TFTP según RFC 1350 (cliente y servidor).
  2. El sistema deberá permitir actualizaciones de software en línea sin necesidad de interrumpir su funcionamiento.
  3. Asimismo deberá permitir realizar una copia de resguardo del sistema actual, a fin de tener la capacidad de recuperarlo en caso de que la actualización no funcione adecuadamente.
- Servicio de configuración por medio de consola remota Telnet según RFCs 854/855 sobre transporte TCP/IP según RFCs 793/791.
- Soporte de replicación o copiado de tráfico configurable, ya sea mediante ACL, port, MAC address o VLAN hacia un puerto específico definido por el administrador para su estudio y análisis.

#### **REDUNDANCIA Y ALTA DISPONIBILIDAD**

- Fuente de alimentación redundante (mínimo 1+1).
- Ventiladores redundantes, reemplazables en caliente.
- Debe poseer la capacidad de stack para datos y permitir tener las fuentes de alimentación dentro del stack trabajando como una fuente común de energía.
- Deberá soportar al menos 8 unidades formando parte de un mismo stack.
- El tráfico dentro del stack debe poseer un bandwidth de como mínimo 450



Gbps.

- Los switches propuestos deberán contar con capacidad de converger una red Wireless y cableada para funcionar como controlador de los puntos de acceso wireless sin el agregado de hardware y mediante licenciamiento opcional.
- El switch propuesto deberá tener la posibilidad de desplegar en un mismo stack, diferentes tecnologías Fibre/Cobre.

ETSWL2PS48GB

#### **Conmutador (Switch) de Core Modular**

Concentrador Switch de Core Modular con las siguientes características:

- Concentrador Switch para conmutación de tramas LAN.
- Deberá contar con servicios de red de capa 2 (network layer 2).
- Deberá contar con “stack dual” IPv4/IPv6.
- Deberá incluir los accesorios necesarios para montar en racks estándar de 19”.
- Debe ocupar una altura no superior a <1> unidades de rack.
- Cada unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados en formato papel o mediante medios de almacenamiento

271



digitales.

- Puertos adicionales 2 x 10G SFP + LAN base
- Los equipos deberán ser alimentados de 220 V - 50 Hz, monofásico con toma de 3 patas planas, sin necesidad de requerir un transformador adicional.
- Compatibilidad mínima: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet en cobre (IEEE 802.3ab), Gigabit Ethernet en fibra (IEEE 802.3z)

#### CONECTIVIDAD

- La cantidad de puertos de concentración inicial deberá proveerse mediante la instalación de los módulos correspondientes para los tipos indicados en la tabla que se incluye más abajo.
- En caso de que el acceso a la interfaz física sea implementada mediante transceptores enchufables, los mismos deberán ser del tipo SFP o similar.
- Cantidad y tipo de bocas mínimo a incluir en el switch:

Tipo	Cantidad	PoE
1000 Base	48	SI

- Todos los puertos de cobre 10/100BaseT ó 10/100/1000BaseT deberán soportar la característica Auto-MDIX, es decir el conector deberá ajustar automáticamente su funcionamiento sin importar si se enchufa un cable



directo o uno cruzado.

- Para modo full dúplex los puertos deberán soportar control de flujo mediante IEEE 802.3X.
- Todos los puertos deberán soportar IEEE 802.3ad LACP (Link Aggregation Control Protocol) para agrupamiento de enlaces en un único canal de mayor ancho de banda.
- Los puertos de cobre que incluyan la característica PoE (Power Over Ethernet) IEEE 802.3af, deberán contar con una potencia no inferior a 15,4 W por boca. (740 W)
- Para los puertos de cobre para los que se solicita la funcionalidad PoE, la misma deberá ser concurrente, es decir, el equipo deberá ser capaz de alimentar la totalidad de los puertos solicitados de manera simultánea, aun cuando para cumplir con este requerimiento se deba agregar fuentes de alimentación adicionales o de mayor potencia.

#### **CAPACIDADES DE CAPA 2 (LAYER 2)**

- Soporte de al menos 32000 MAC address de red.
- Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en cualquier puerto según IEEE 802.1 p/Q o por reglas de asignación por port y address MAC.
- Deberá soportar no menos de 255 VLANs, con posibilidad de escalar a 4000 mediante upgrade de software y/o licencia.
- Soporte de Spanning Tree Protocol según IEEE 802.1D y Rapid Spanning Tree Protocol según IEEE 802.1w.



- Soporte de Multiple Spanning Tree Protocol según IEEE 802.1s para mejorar la eficiencia de convergencia en entornos VLAN.

#### **CALIDAD DE SERVICIO (QoS)**

- Deberá implementar mecanismos para clasificación de tráfico tanto en IPv4 como IPv6.
- Deberá poseer al menos 8 colas de priorización de tráfico por puerto, y al menos una de las colas deberá tener prioridad absoluta en la conmutación de su tráfico por sobre todas las demás, esto es, mientras esta cola tenga tráfico en espera, no podrá procesarse ninguna otra cola.
- Permitirá el manejo de políticas de QoS con criterios asignables sobre layer 2 (mínimo).
- Deberá poder realizar mapeos 802.1p/Q a DiffServ/ToS y DiffServ/ToS a 802.1p/Q.

#### **SEGURIDAD**

- Manejo de Listas de Control de Acceso (ACL) sobre layer 2 (mínimo).
- Soporte de autenticación IEEE 802.1x
- Soporte de autenticación múltiple (multi-host) IEEE 802.1x
- Soporte de administración encriptada mediante SNMPv3, SSL o SSH.



## ADMINISTRACIÓN

- Se deberán proveer en un medio extraíble todos los bloques de información de management (MIBs) necesarios.
- Capacidad de soportar al menos 4 grupos de RMON.
- Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con las siguientes características:
  1. El sistema deberá permitir actualizaciones de software en línea sin necesidad de interrumpir su funcionamiento.
  2. Asimismo deberá permitir realizar una copia de resguardo del sistema actual, a fin de tener la capacidad de recuperarlo en caso de que la actualización no funcione adecuadamente.
- Soporte de replicación o copiado de tráfico configurable, ya sea mediante ACL, port, MAC address o VLAN hacia un puerto específico definido por el administrador para su estudio y análisis.

## REDUNDANCIA Y ALTA DISPONIBILIDAD

- Fuente de alimentación redundante (mínimo 1+1).
- Ventiladores redundantes, reemplazables en caliente.
- Debe poseer la capacidad de stack para datos y permitir tener las fuentes de alimentación dentro del stack trabajando como una fuente común de energía.
- Deberá soportar al menos 8 unidades formando parte de un mismo stack.
- El tráfico dentro del stack debe poseer un bandwidth de como mínimo 450



Gbps.

- Debe poder realizar terminación local de túneles CAPWAP (RFC 5416) para permitir la convergencia con los puntos de acceso wireless.
- El switch propuesto deberá tener la posibilidad de desplegar en un mismo stack, diferentes tecnologías Fibre/Cobre.
- Posibilidad de realizar clasificación de tráfico para aplicar políticas de QoS por Access Point, SSID o radio.
- Deberá poseer al menos 4 colas de priorización de tráfico por puerto de Access Point.

ETSWL2PS24GB

#### **Conmutador (Switch) de Core Modular**

Concentrador Switch de Core Modular con las siguientes características:

- Concentrador Switch para conmutación de tramas LAN.
- Deberá contar con servicios de red de capa 2 (network layer 2).
- Deberá contar con "stack dual" IPv4/IPv6.
- Deberá incluir los accesorios necesarios para montar en racks estándar de 19".
- Debe ocupar una altura no superior a <1> unidades de rack.
- Cada unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados en formato papel o mediante medios de almacenamiento

276



digitales.

- Puertos adicionales 4 x 1G SFP + LAN base
- Los equipos deberán ser alimentados de 220 V - 50 Hz, monofásico con toma de 3 patas planas, sin necesidad de requerir un transformador adicional.
- Compatibilidad mínima: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet en cobre (IEEE 802.3ab), Gigabit Ethernet en fibra (IEEE 802.3z)

#### CONECTIVIDAD

- La cantidad de puertos de concentración inicial deberá proveerse mediante la instalación de los módulos correspondientes para los tipos indicados en la tabla que se incluye más abajo.
- En caso de que el acceso a la interfaz física sea implementada mediante transceptores enchufables, los mismos deberán ser del tipo SFP o similar.
- Cantidad y tipo de bocas mínimo a incluir en el switch:

Tipo	Cantidad	PoE
1000 Base	24	SI

- Todos los puertos de cobre 10/100BaseT ó 10/100/1000BaseT deberán soportar la característica Auto-MDIX, es decir el conector deberá ajustar automáticamente su funcionamiento sin importar si se enchufa un cable



directo o uno cruzado.

- Para modo full dúplex los puertos deberán soportar control de flujo mediante IEEE 802.3X.
- Todos los puertos deberán soportar IEEE 802.3ad LACP (Link Aggregation Control Protocol) para agrupamiento de enlaces en un único canal de mayor ancho de banda.
- Los puertos de cobre que incluyan la característica PoE (Power Over Ethernet) IEEE 802.3af, deberán contar con una potencia no inferior a 15,4 W por boca. ( 370 W)
- Para los puertos de cobre para los que se solicita la funcionalidad PoE, la misma deberá ser concurrente, es decir, el equipo deberá ser capaz de alimentar la totalidad de los puertos solicitados de manera simultánea, aun cuando para cumplir con este requerimiento se deba agregar fuentes de alimentación adicionales o de mayor potencia.

#### **CAPACIDADES DE CAPA 2 (LAYER 2)**

- Soporte de al menos 32000 MAC address de red.
- Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en cualquier puerto según IEEE 802.1 p/Q o por reglas de asignación por port y address MAC.
- Deberá soportar no menos de 255 VLANs, con posibilidad de escalar a 4000 mediante upgrade de software y/o licencia.
- Soporte de Spanning Tree Protocol según IEEE 802.1D y Rapid Spanning Tree Protocol según IEEE 802.1w.



- Soporte de Multiple Spanning Tree Protocol según IEEE 802.1s para mejorar la eficiencia de convergencia en entornos VLAN.

#### **CALIDAD DE SERVICIO (QoS)**

- Deberá implementar mecanismos para clasificación de tráfico tanto en IPv4 como IPv6.
- Deberá poseer al menos 8 colas de priorización de tráfico por puerto, y al menos una de las colas deberá tener prioridad absoluta en la conmutación de su tráfico por sobre todas las demás, esto es, mientras esta cola tenga tráfico en espera, no podrá procesarse ninguna otra cola.
- Permitirá el manejo de políticas de QoS con criterios asignables sobre layer 2 (mínimo).
- Deberá poder realizar mapeos 802.1p/Q a DiffServ/ToS y DiffServ/ToS a 802.1p/Q.

#### **SEGURIDAD**

- Manejo de Listas de Control de Acceso (ACL) sobre layer 2 (mínimo).
- Soporte de autenticación IEEE 802.1x
- Soporte de autenticación múltiple (multi-host) IEEE 802.1x
- Soporte de administración encriptada mediante SNMPv3, SSL o SSH.



## ADMINISTRACIÓN

- Se deberán proveer en un medio extraíble todos los bloques de información de management (MIBs) necesarios.
- Capacidad de soportar al menos 4 grupos de RMON.
- Almacenamiento de sistema operativo y configuración en memoria Flash reescribible con las siguientes características:
  1. El sistema deberá permitir actualizaciones de software en línea sin necesidad de interrumpir su funcionamiento.
  2. Asimismo deberá permitir realizar una copia de resguardo del sistema actual, a fin de tener la capacidad de recuperarlo en caso de que la actualización no funcione adecuadamente.
- Soporte de replicación o copiado de tráfico configurable, ya sea mediante ACL, port, MAC address o VLAN hacia un puerto específico definido por el administrador para su estudio y análisis.



### **REDUNDANCIA Y ALTA DISPONIBILIDAD**

- Fuente de alimentación redundante (mínimo 1+1).
- Ventiladores redundantes, reemplazables en caliente.
- Debe poseer la capacidad de stack para datos y permitir tener las fuentes de alimentación dentro del stack trabajando como una fuente común de energía.
- Deberá soportar al menos 8 unidades formando parte de un mismo stack.
- El tráfico dentro del stack debe poseer un bandwidth de como mínimo 450 Gbps.
- Debe poder realizar terminación local de túneles CAPWAP (RFC 5416) para permitir la convergencia con los puntos de acceso wireless.
- El switch propuesto deberá tener la posibilidad de desplegar en un mismo stack, diferentes tecnologías Fibre/Cobre.
- Posibilidad de realizar clasificación de tráfico para aplicar políticas de QoS por Access Point, SSID o radio.
- Deberá poseer al menos 4 colas de priorización de tráfico por puerto de Access Point

### **EQUIPAMIENTO SERVICIOS CENTRALES**



## CONDICIONES PARTICULARES ESPECIFICAS – APLICA A TODOS LOS ITEM'S

CONDICIONES PARTICULARES ESPECÍFICAS	
<b>A - Marca de Fábrica</b>	
•	Los bienes ofrecidos deberán poseer una única marca de fábrica, y ser la empresa fabricante la propietaria de dicha marca, la que deberá acreditar en forma fehaciente tal situación.
•	La marca de fábrica de los bienes deberá pertenecer a empresas reconocidas como sociedades comerciales en la República Argentina de acuerdo a la Ley n° 19.550, las cuales podrán ser empresas subsidiarias o controladas o pertenecientes al grupo económico dueño de la marca de fábrica, contando como mínimo con 5 años de radicación en el país.
<b>B - Respecto de los bienes ofertados</b>	
•	<i>Cumplimiento de Norma ISO 900X</i>
•	El fabricante del equipo ofertado deberá cumplir con la norma ISO 900X desarrollada por la International Standards Organization, para el proceso de producción del equipo solicitado.
•	Si los procesos de fabricación y ensamblado se ejecutan en plantas diferentes, cada planta deberá cumplir con la certificación ISO 900X para los procesos mencionados.
•	Deberá presentar conjuntamente con la Oferta copia autenticada de la/s certificación/es exigida/s vigente/s y expedida/s a favor del fabricante del equipo.
•	El Oferente deberá en su Oferta a título de Declaración Jurada, informar si el origen de los bienes, son de las plantas certificadas y



	cuyas copias autenticadas de las respectivas certificaciones forman parte de la Oferta.
•	<i>Cumplimiento de Norma ISO 14001</i>
	La empresa fabricante del bien ofertado deberá cumplir con la norma ISO 14001 desarrollada por la International Standards Organization. Deberá presentar conjuntamente con la Oferta copia autenticada de la certificación vigente y expedida a favor del fabricante del equipo.
•	Memorias, disketteras y discos rígidos, deberán ser provistos por la empresa fabricante del bien ofrecido. En el caso de no ser de la misma marca de fábrica de dicho bien deberán contar con sello inalterable de control de calidad de dicho fabricante. En el momento de recepcionar los equipos se constatará lo antedicho, con el procedimiento que el área informática encargada de la recepción considere conveniente
•	La marca de fábrica de la CPU debe ser la misma que la de la Placa Madre.
•	Si el monitor es fabricado por un tercero por cuenta y orden de la empresa propietaria de la marca de los bienes, deberá presentar conjuntamente con la Oferta, copia autenticada del contrato de fabricación.
•	El bien ofertado deberá estar en producción al momento de la apertura de Ofertas.  Si se dejara de comercializar el bien durante el período entre la presentación de la Oferta y el perfeccionamiento del contrato, la empresa adjudicataria deberá reemplazarlo por el comercializado, el que deberá poseer características técnicas iguales o superiores al ofertado.  Ese reemplazo deberá ser previamente autorizado por la Dirección Provincial de Sistemas de Información y Tecnologías.



	<p>La DPSIT podrá autorizar los cambios en razón de avances tecnológicos que se produjeran en cualquiera de las partes o componentes del equipamiento durante el período de aprovisionamiento o como consecuencia de proveer un nuevo equipo según lo establecido por las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: <b>Defectos de Origen - Vicios de Fabricación – Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía</b> –, siempre que dichos avances tecnológicos no modifiquen el objetivo por el que fue adquirido el bien y mantengan o mejoren la prestación del equipamiento.</p>
•	<p>La identificación de marca, modelo y número de serie del equipo y el monitor deberán ser inviolables, es decir, de calidad tal que imposibilite su remoción y que no pueda ser adulterado, en ambos casos, sin dejar evidencias.</p>
•	<p>El bien ofertado deberá cumplir con las especificaciones técnicas básicas, será nuevo, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso a que el Comprador será el primer usuario del bien desde su fabricación).</p>
•	<p>El oferente deberá garantizar que no existirán limitaciones para que la Superintendencia de Entidades Financieras y Cambiarias tenga acceso a toda documentación técnica relacionada y a la realización de auditorías periódicas en las instalaciones del proveedor.</p>
<p><b>C - Respecto a la presentación de Ofertas</b></p>	
•	<p>La Oferta deberá ser presentada por escrito respetando el orden impuesto en las “<b>Especificaciones Técnicas Básicas</b>”, incluyendo la descripción técnica, en cada uno de los puntos solicitados (leyenda “Especificar”) en forma clara, detallada, precisa y sin ambigüedades. No se admitirá ni se considerará como especificación, descripción o identificación del bien ofrecido leyendas “según pliego” o expresiones de índole similar o</p>



	referencias a folletos adjuntos.
•	Se deberá adjuntar toda la documentación indicada y establecida en las <b>“<u>Condiciones Particulares Específicas</u>”</b> y las <b>“<u>Especificaciones Técnicas Básicas</u>”</b> .
•	Se podrá, a los fines de lograr una mejor comprensión de las especificaciones consignadas, incluir folletos técnicos (o información impresa proveniente del sitio oficial de la empresa fabricante) de los equipos y los periféricos asociados, pudiendo ser presentados en idioma español o en idioma inglés. Se deja establecido que los folletos adjuntos no forman parte de la Oferta
<b>D - Respecto a la Evaluación de Ofertas</b>	
•	<p>Evaluación de la documentación presentada</p> <ul style="list-style-type: none"> <li>Se evaluará que se haya presentado la documentación requerida en las <b>“<u>Condiciones Particulares Específicas</u>”</b> y las <b>“<u>Especificaciones Técnicas Básicas</u>”</b>. De existir faltantes, la Oferta será declara <b>“<u>No admisible técnicamente</u>”</b></li> </ul> <p>Se verificará la validez y consistencia de dicha documentación.</p> <ul style="list-style-type: none"> <li>Se verificará que el bien ofrecido cumpla con las <b>“<u>Condiciones Particulares Específicas</u>”</b> y las <b>“<u>Especificaciones Técnicas Básicas</u>”</b> . En caso que no cumpla, la Oferta será declarada <b>“<u>No admisible técnicamente</u>”</b>.</li> </ul> <p>3. El comitente podrá solicitar aclaraciones, a través de notificación fehaciente, donde se establecerá el plazo otorgado para dar respuesta.</p>



### E - Recepción de bienes

- El Adjudicatario deberá proveer los manuales técnicos y de usuario originales (no siendo permitido la presentación de fotocopias) correspondientes a los bienes entregados, preferentemente en castellano o en su defecto en inglés
- El Adjudicatario deberá proveer todos los cables y elementos necesarios para el correcto funcionamiento del bien.

### F - Garantía de los bienes

- - Garantía.
    1. Los bienes suministrados tendrán una garantía de la empresa fabricante por un término mínimo de 36 meses, la cual deberá mantenerse, sin perjuicio de la apertura de la CPU, sin que para ello sea necesario solicitar autorización al proveedor y/o empresa fabricante.
    2. Garantía de buen funcionamiento:
      1. En el caso del hardware, la "Garantía de buen funcionamiento" abarcará todo el período indicado en el Punto 1.1 y deberá cumplir los siguientes requisitos:
        1. La presente garantía incluirá el servicio de reparación por personal calificado con la provisión y el reemplazo de las partes que se encuentren defectuosas por repuestos originales. Los elementos reemplazantes deberán ser de las mismas características o en su defecto equivalentes en su rendimiento según las pautas de calidad



establecidas por el fabricante original del bien entregado. Deberá presentarse, en caso de ser requerido, la documentación que respalde lo previamente expuesto.

2. A efectos de cumplimentar con el servicio de garantía, el equipamiento se centralizará en una dependencia del Organismo Contratante, la cual podrá ser establecida dentro de la ciudad de La Plata y su área de influencia y la Ciudad Autónoma de Buenos Aires, donde la empresa fabricante deberá repararlo o retirarlo para su reparación. Los gastos de traslado desde y hacia esa dependencia estarán a cargo exclusivo del proveedor. (Se define al área de influencia de la ciudad de La Plata a los partidos de La Plata, Berisso y Ensenada).
3. La reparación de los bienes deberá ser ejecutada a satisfacción del Comprador. El tiempo de respuesta entre el pedido de reparación y el inicio de la misma no podrá superar las 4 hs. El tiempo máximo de reparación será de 48 hs. El horario disponible para reclamos deberá ser de 9.00 hs. a 18 hs.

Se define "El tiempo de respuesta entre el pedido de reparación y el inicio de la misma" al tiempo máximo que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y la asistencia remota o presencial de personal técnico idóneo con el fin de determinar la



avería en el equipo afectado.

Se define “El tiempo máximo de reparación” al lapso que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y el momento en que el organismo recepciona y verifica el buen funcionamiento del bien afectado.

4. La cantidad de días de indisponibilidad, según se define en las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: **Defectos de Origen - Vicios de Fabricación - Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía** –, se establece en quince (15) días.

#### ETSRVBPRACK – SERVIDOR BI-PROC RACK

ESPECIFICACIONES TECNICAS BASICAS – ITEM 1

Cantidad: Uno (1)



Marca del Equipo:	
Modelo del Equipo:	
Chasis - Fuente	
Factor de forma:	
Diseño modular basado en un chasis para montar en Racks normalizados de 19". Factor de forma: 2U	
El chasis del computador deberá contar como mínimo con seis bahías libres para discos Hot-Swap, previo a la instalación de los discos requeridos.	
La fuente del computador deberá tener la potencia necesaria para garantizar el correcto funcionamiento de la unidad a su máxima configuración.	
Deberá proveerse con fuente de poder redundante intercambiable en caliente.	
El equipo deberá incluir ventilación interna redundante y reemplazable en caliente, de forma tal que si alguno de los ventiladores del sistema principal de enfriamiento interno presente una avería, el equipo continúe funcionando, debiendo existir algún mecanismo de alerta de la falla producida	
Procesador	



Arquitectura de procesamiento múltiple simétrico (SMP) con capacidad de hasta 2 procesadores.  Se proveerá con 2 (dos) procesadores Intel Xeon línea E5 2600 v3 o superior con dieciocho (18) cores como mínimo cada uno.  La memoria secundaria o caché corresponderá ser la que por defecto viene integrada con el microprocesador
<b>Bus</b>
El bus del computador deberá ser de arquitectura PCI / PCI Express
Deberá contar como mínimo con tres slots PCI Express G3.
<b>Memoria RAM</b>
Marca:
Modelo o Número de Parte:
Provisión : mínimo 128 Gb.
Tipo : DDR4 ECC o superior
Ampliación : Mínimo 384 Gb.
La cantidad de módulos a proveer deberá estar en configuración óptima según el microprocesador ofertado y sus canales.
<b>Sistema de almacenamiento</b>
Arreglo de disco:
Sistema de arreglo de discos:
Sistema de disk array Serial Attached SCSI visible como una



unidad lógica de 2Tb.en RAID 1

Controladora de arreglo: deberá contar con 64 Mbytes mínimo de memoria cache de disco con batería de resguardo y deberá cumplir con las especificaciones para RAID 0, 1; contando con la capacidad de ante una eventual avería el sistema alerte al operador (a través de un software apropiado por pantalla y/o una señal luminosa relacionada al dispositivo con problemas) para poder realizarse el reemplazo por otro provisto por el oferente como repuesto para ese propósito incluido en la oferta, sin necesidad de detener el equipo (hot pluggable) y con actualización automática de datos.

Los discos provistos serán de tecnología SAS con factor de forma de 3.5" (Mínimo en cantidad: 3 - tres)

Se proveerán los drivers necesarios para el correcto funcionamiento de esta unidad bajo el sistema operativo indicado.

Controladora de arreglo:

Marca:

Modelo o Número de Parte:

Discos:

Marca:

Modelo o Número de Parte:

Cantidad:

Unidad lectora de DVD-ROM interna

Marca:



Modelo o Número de Parte:	
Velocidad mínima de lectura de DVD-ROM: 8x	
Deberá soportar las normas. CD-ROM, CD-R, DVD-ROM y DVD-R o DVD+R	
Se suministrarán los drivers correspondientes para su correcto funcionamiento bajo el sistema operativo indicado	
<b>Controlador de Video</b>	
Controlador de video integrado con resolución de 1024 x 768 o 1440 x 900 pixels. Un puerto frontal y uno trasero	
<b>Interfaces integrada en la placa madre</b>	
Deberá poseer dos (2) puertos USB frontales y dos (2) puertos USB traseros. Al menos uno de cada ubicación compatible con USB 3 .	
<b>Dispositivo de Red</b>	
Cantidad: 4 – cuatro. Se deberán incluir, como mínimo, dos controladores y/o placas de red independientes.	
Capacidad para conectarse a una red local (LAN) tipo Ethernet/IEEE 802.3 / Fast Ethernet/IEEE 802.3u / Gigabit Ethernet 802.3ab autoswitchable	
Soporte de medio físico 10/100/1000 Base-TX	
Conector: RJ45	
Se proveerán los manejadores de dispositivo para su correcto funcionamiento bajo el sistema operativo indicado	



Varios	
Interface para consola remota por red con capacidad de encendido, monitoreo, administración y diagnóstico del servidor.  Se deberá proveer el software y, en caso que aplicara, las licencias necesarias para poder utilizar la plena funcionalidad de dicha interface de administración remota según los sistemas operativos indicados en el punto "Drivers / Controladores"	
Sistema Operativo	
Se cotizará sin sistema operativo	
Compatibilidad	
Los componentes incluidos en el bien del presente Renglón deberán ser compatibles con el sistema operativo Linux kernel 2.6 o superior (Linux Debian y/o RedHat Enterprise) y Windows 2008 Server y versiones posteriores. También deberán ser compatibles con software de virtualización VMware ESX Server 5.0 y superiores.	
Drivers / Controladores	
Con el equipo se deberán proveer los drivers/controladores necesarios para el correcto funcionamiento del equipo bajo Linux y Windows 2008 Server y versiones posteriores.  El presente requerimiento se basa en la posibilidad que en etapa posterior a la presente tramitación el Organismo instale alguno de los sistemas operativos indicados.	

**ETSRVMPRACK – SERVIDOR MONO-PROC RACK**

293

PLIEG-2017-05863125-GDEBA-DJLIPLYC



<b>ESPECIFICACIONES TECNICAS BASICAS</b>	
Marca del Equipo:	
Modelo del Equipo:	
Chasis – Fuente	
Factor de forma:  El chasis del computador deberá contar como mínimo con cuatro bahías de discos rígidos y permitir acceder externamente como mínimo a un medio óptico y una unidad de back-up	Especificar
La fuente del computador deberá tener la potencia necesaria para garantizar el correcto funcionamiento de la unidad a su máxima configuración.	Especificar
Procesador	
Serán aceptables cualquiera de las siguientes opciones	Especificar
<ul style="list-style-type: none"> <li>Arquitectura de procesamiento de 1 procesador Intel Xeon línea E3-1200v2 o superior de cuatro núcleos cada uno como mínimo.</li> </ul> <p>La memoria secundaria o caché corresponderá ser la que por defecto viene integrada con el microprocesador.</p>	
<ul style="list-style-type: none"> <li>Arquitectura de procesamiento de 1 procesador AMD quad-core, línea Opteron o superior.</li> </ul> <p>La memoria secundaria o caché corresponderá ser la que por defecto viene integrada con el microprocesador</p>	



Bus		
	El bus del computador deberá ser de arquitectura PCI / PCI Express	Especificar
	Deberá contar como mínimo con tres slots PCI Express G2.	Especificar
Memoria RAM		
	Marca:	Especificar
	Modelo o Número de Parte:	Especificar
	Provisión : mínimo 16 Gb.	Especificar
	Tipo : DDR3 ECC de 1333Mhz. o superior	Especificar
	Ampliación : Mínimo 32 Gb.	Especificar
Sistema de almacenamiento		
	<b>Arreglo de disco:</b>	Especificar



El equipo poseerá un controlador de arreglo de discos que cumpla la norma Serial ATA (SATA II o SATA 3G) y las especificaciones para RAID 0 y 1.	
<b>Discos:</b>	
Se proveerán dos discos de 500 Gb. de tecnología SATA II o SATA 3G, de 7.500 rpm, como mínimo	
Se proveerán los drivers necesarios para el correcto funcionamiento de esta unidad bajo el sistema operativo indicado	
<b>Controladora de arreglo:</b>	
Marca:	Especificar
Modelo o Número de Parte:	Especificar
<b>Discos:</b>	
Marca:	Especificar
Modelo o Número de Parte:	Especificar
Cantidad:	Especificar
<b>Unidad lectora de DVD-ROM interna</b>	
Marca:	Especificar
Modelo o Número de Parte:	Especificar



	Velocidad mínima de lectura de DVD-ROM: 8x	Especificar
	Deberá soportar las normas. CD-ROM, CD-R, DVD-ROM y DVD-R o DVD+R	Especificar
	Se suministrarán los drivers correspondientes para su correcto funcionamiento bajo el sistema operativo indicado	Especificar
<b>Controlador de Video</b>		
	Controlador de video integrado o placa PCI Express con resolución de 1024 x 768 o 1440 x 900 pixels.	Especificar
<b>Interfaces integrada en la placa madre</b>		
	Serán aceptables cualquiera de las siguientes opciones	Especificar
	<ul style="list-style-type: none"> <li>Un puerto serie RS-232 del tipo 16550A, un puerto para la conexión del bus mouse, un puerto para conexión al teclado y cuatro puertos USB (compatible con USB 2.0).</li> </ul>	
	<ul style="list-style-type: none"> <li>Un puerto serie RS-232 del tipo 16550A y cuatro puertos USB (compatible con USB 2.0). Deberá proveerse un adaptador USB-PS/2 con soporte para teclado y mouse.</li> </ul>	
<b>Unidad de back-up</b>		
	Unidad de tape back-up, con capacidad por cartridge de por lo menos 800 GB. sin compresión.	Especificar
	Conexión : SAS o SATA	Especificar
	Se proveerán los drivers compatibles con el sistema operativo solicitado y el software necesario para realizar backup automático y la administración de la unidad desde una red local (LAN)	Especificar



Dispositivo de Red		
	Cantidad : 2 – dos	Especificar
	Capacidad para conectarse a una red local (LAN) tipo Ethernet/IEEE 802.3 / Fast Ethernet/IEEE 802.3u / Gigabit Ethernet 802.3ab autoswitchable	Especificar
	Soporte de medio físico 10 Base-T/100 Base-TX / 1000 Base Tx	Especificar
	Conexión UTP con conector RJ 45	
	Se proveerán los manejadores de dispositivo para su correcto funcionamiento bajo el sistema operativo indicado	Especificar
Sistema Operativo		
	Se cotizará sin sistema operativo	
Compatibilidad		
	Los componentes incluidos en el bien del presente Renglón deberán ser compatibles con el sistema operativo Linux kernel 2.6 o superior (Linux Debian y/o RedHat Enterprise) y Windows 2003 Server y versiones posteriores. También deberán ser compatibles con software de virtualización como VMware ESX Server, Citrix XenServer y Microsoft Virtual Server.	Especificar
Drivers / Controladores		



	<p>Con el equipo se deberán proveer los drivers/controladores necesarios para el correcto funcionamiento del equipo bajo Linux y Windows 2003 Server y versiones posteriores.</p> <p>El presente requerimiento se basa en la posibilidad que en etapa posterior a la presente tramitación un Organismo instale alguno de los sistemas operativos indicados.</p>	Especificar
Insumos		
	Se deberán proveer 10 cintas compatibles con la unidad incluida en el presente servidor.	Especificar

## EQUIPAMIENTO DESKTOP

### ETPCSMLF – PC SMALL FACTOR

CONDICIONES PARTICULARES ESPECÍFICAS	
<b>A - Marca de Fábrica</b>	
•	Los bienes ofrecidos deberán poseer una única marca de fábrica, y ser la empresa fabricante la propietaria de dicha marca, la que deberá acreditar en forma fehaciente tal situación.
•	La marca de fábrica de los bienes deberá pertenecer a empresas reconocidas como sociedades comerciales en la República Argentina de acuerdo a la Ley n° 19.550, las cuales podrán ser empresas subsidiarias o controladas o pertenecientes al grupo económico dueño de la marca de fábrica, contando como mínimo con 5 años de radicación en el país.
<b>B - Respetto de los bienes ofertados</b>	



•	<i>Cumplimiento de Norma ISO 900X</i>
	<ul style="list-style-type: none"> <li>El fabricante del equipo ofertado deberá cumplir con la norma ISO 900X desarrollada por la International Standards Organization, para el proceso de producción del equipo solicitado. Deberá presentar conjuntamente con la Oferta copia autenticada de la certificación vigente y expedida a favor del fabricante del equipo.</li> </ul>
	<ul style="list-style-type: none"> <li>El monitor deberá ser fabricado en planta que acredite el cumplimiento del estándar ISO 900X, debiendo adjuntarse a la Oferta copia autenticada de dicha certificación.</li> </ul>
	<ul style="list-style-type: none"> <li>El Oferente deberá en su Oferta a título de Declaración Jurada, informar si el origen de los bienes, son de las plantas certificadas y cuyas copias autenticadas de las respectivas certificaciones forman parte de la Oferta.</li> </ul>
•	Si el monitor es fabricado por un tercero por cuenta y orden de la empresa propietaria de la marca de los bienes, deberá presentar conjuntamente con la Oferta, declaración jurada de tal situación con el aval de ambas partes.
•	Todos los componentes del equipo deberán ser provistos por la empresa fabricante.
•	<p>El bien ofertado, como así también los componentes que lo conforman, deberán estar en producción al momento de la apertura de Ofertas.</p> <p>Si se dejara de comercializar el equipo y/o los componentes que lo conforman durante el período entre la presentación de la Oferta y el perfeccionamiento del contrato, la empresa adjudicataria deberá reemplazarlo por el comercializado, el que deberá poseer características técnicas y rendimiento de performance igual o superior al ofertado.</p>



	<p>Ese reemplazo deberá ser previamente autorizado por la Dirección Provincial de Sistemas de Información y Tecnologías.</p> <p>La DPSIT podrá autorizar los cambios en razón de avances tecnológicos que se produjeran en cualquiera de las partes o componentes del equipamiento durante el período de aprovisionamiento o como consecuencia de proveer un nuevo equipo según lo establecido por las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: <b>Defectos de Origen - Vicios de Fabricación – Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía</b> –, siempre que dichos avances tecnológicos no modifiquen el objetivo por el que fue adquirido el bien y mantengan o mejoren la prestación del equipamiento.</p>
<ul style="list-style-type: none"> <li>•</li> </ul>	<p>La identificación de marca, modelo y número de serie del equipo y periféricos deberán ser inviolables, es decir, de calidad tal que imposibilite su remoción y que no pueda ser adulterado, en ambos casos, sin dejar evidencias.</p>
<ul style="list-style-type: none"> <li>•</li> </ul>	<p>El bien ofertado deberá cumplir con las especificaciones técnicas básicas, será nuevo, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso a que el Comprador será el primer usuario del bien desde su fabricación).</p>
<p><b>C - Respecto a la presentación de Ofertas</b></p>	
<ul style="list-style-type: none"> <li>•</li> </ul>	<p>La Oferta deberá ser presentada por escrito respetando el orden impuesto en las <b>“Especificaciones Técnicas Básicas”</b>, describiendo técnicamente cada uno de los puntos solicitados (leyenda “Especificar”), en forma clara, detallada, precisa y sin ambigüedades. No se admitirá ni se considerará como especificación, descripción o identificación del bien ofrecido leyendas del tipo “según pliego” o expresiones de índole similar o referencias a folletos adjuntos.</p>



•	Se deberá adjuntar toda la documentación indicada y establecida en las <b>“<u>Condiciones Particulares Específicas</u>”</b> y las <b>“<u>Especificaciones Técnicas Básicas</u>”</b> .
•	Se podrá, a los fines de lograr una mejor comprensión de las especificaciones consignadas, incluir folletos técnicos (o información impresa proveniente del sitio oficial de la empresa fabricante) de los equipos, de sus componentes y los periféricos asociados, pudiendo ser presentados en idioma español o en idioma inglés. Se deja establecido que los folletos adjuntos no forman parte de la Oferta.
<b>D - Respecto a la Evaluación de Ofertas</b>	
•	<p>Evaluación de la documentación presentada</p> <ul style="list-style-type: none"> <li>• Se evaluará que se haya presentado la documentación requerida en las <b>“<u>Condiciones Particulares Específicas</u>”</b> y las <b>“<u>Especificaciones Técnicas Básicas</u>”</b>. De existir faltantes, la Oferta será declara <b>“<u>No admisible técnicamente</u>”</b></li> </ul> <p>Se verificará la validez y consistencia de dicha documentación.</p> <ul style="list-style-type: none"> <li>• Se verificará que el bien ofrecido cumpla con las <b>“<u>Condiciones Particulares Específicas</u>”</b> y las <b>“<u>Especificaciones Técnicas Básicas</u>”</b> . En caso que no cumpla, la Oferta será declarada <b>“<u>No admisible técnicamente</u>”</b>.</li> </ul>
•	El comitente podrá solicitar aclaraciones, a través de notificación fehaciente, donde se establecerá el plazo otorgado para dar respuesta.
<b>E - Recepción de bienes</b>	



•	El Comitente contará con un plazo de 30 días corridos, a partir de la fecha de recepción de los bienes, para constatar que los mismos cumplan con lo especificado en la Oferta y/o con la evaluación resultante del punto anterior, conforme lo establecido en el Artículo 65 del Decreto n° 3300/72 (T.O. 2004).
•	El Adjudicatario deberá proveer los manuales técnicos y de usuario originales (no siendo permitido la presentación de fotocopias) correspondientes a los bienes entregados, preferentemente en castellano o en su defecto en inglés.
•	El Adjudicatario deberá proveer los cables necesarios para la correcta instalación y funcionamiento del bien.
<b>F - Garantía de los bienes</b>	
•	<ul style="list-style-type: none"> <li>• Garantía.             <ol style="list-style-type: none"> <li>1. Los bienes suministrados tendrán una garantía de la empresa fabricante por un término mínimo de 36 meses, la cual deberá mantenerse, sin perjuicio de la apertura de la CPU, sin que para ello sea necesario solicitar autorización al proveedor y/o empresa fabricante.</li> <li>2. Garantía de buen funcionamiento:                 <ol style="list-style-type: none"> <li>1. En el caso del hardware, la “Garantía de buen funcionamiento” abarcará todo el período indicado en el Punto 1.1 y deberá cumplir los siguientes requisitos:                     <ol style="list-style-type: none"> <li>1. La presente garantía incluirá el servicio de reparación por personal calificado con la provisión y el reemplazo de las partes que se encuentren defectuosas por repuestos</li> </ol> </li> </ol> </li> </ol> </li> </ul>



originales. Los elementos reemplazantes deberán ser de las mismas características o en su defecto equivalentes en su rendimiento según las pautas de calidad establecidas por el fabricante del bien entregado y las exigidas en las “Especificaciones Técnicas Básicas”. Deberá presentarse, en caso de ser requerido, la documentación que respalde lo previamente expuesto.

2. A efectos de cumplimentar con el servicio de garantía, el equipamiento se centralizará en una dependencia del Organismo Contratante, la cual podrá ser establecida dentro de la ciudad de La Plata y su área de influencia, la Ciudad Autónoma de Buenos Aires, donde la empresa fabricante deberá repararlo o retirarlo para su reparación. Los gastos de traslado desde y hacia esa dependencia estarán a cargo exclusivo del proveedor. (Se define al área de influencia de la ciudad de La Plata a los partidos de La Plata, Berisso y Ensenada).
3. La reparación de los bienes deberá ser ejecutada a satisfacción del Comprador. El tiempo de respuesta entre el pedido de reparación y el inicio de la misma no podrá superar las 24 hs. El tiempo máximo de reparación será de siete (7) días. El horario disponible para reclamos deberá ser de 9.00



hs. a 18 hs.

Se define “El tiempo de respuesta entre el pedido de reparación y el inicio de la misma” al tiempo máximo que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y la presencia de personal técnico idóneo con el fin de determinar la avería en el equipo afectado.

Se define “El tiempo máximo de reparación” al lapso que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y el momento en que el organismo recepciona y verifica el buen funcionamiento del bien afectado.

4. La cantidad de días de indisponibilidad, según se define en las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: **Defectos de Origen - Vicios de Fabricación - Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía** –, se establece en sesenta (60) días.

**PC formato Small para atención en Cajas con Sistema operativo y Monitor LED**

<b>ESPECIFICACIONES TECNICAS BASICAS</b>
--

<b>Marca del Equipo:</b>
--------------------------



<b>Modelo del Equipo:</b>	
<b>Gabinete – Fuente</b>	
Factor de forma:  Se admitirán gabinetes con formato SFF (small form Factor) dos puertos USB accesibles desde el exterior como mínimo  Seguridad: El gabinete deberá contar con un dispositivo de seguridad tal que permita bloquear su apertura sea a través de algún mecanismo tipo pestaña o solapa de seguridad para precintar.	Especificar
La fuente de alimentación deberá corresponder a las normativas de seguridad y tensión de red de la República Argentina, y proporcionar la potencia necesaria para el correcto funcionamiento de la unidad en su máxima configuración.	Especificar
<b>Placa Madre</b>	
Marca:	Especificar
Modelo:	Especificar
Chipset:	Especificar
La interconexión de componentes deberá ser resuelta dentro del propio gabinete.	Especificar
<b>Características Generales:</b>	



<p>Arquitectura x86 con soporte USB (Universal Serial Bus) Setup residente en ROM con password de booteo y setup.</p> <p>(Acceso desbloqueado a bios setup).</p> <p>Control de booteo residente en ROM, con posibilidad de booteo desde DVD-ROM, CD-ROM y/o dispositivo USB.</p> <p>Capacidad de booteo remoto a través de la conexión LAN.</p> <p>Reloj en tiempo real con batería y alarma audible. Deberán indicarse otros controles adicionales que posea.</p>	
Actualización BIOS	
<p>La actualización del BIOS del equipo deberá poder realizarse mediante la descarga de software de la Web de la empresa fabricante.</p>	Especificar
Procesador	
<p>Basada en registros de 32 bits o superior, totalmente compatible con alguna de las siguientes arquitecturas:</p> <ul style="list-style-type: none"> <li>- Intel Core i3 (4ta generacion) o superior</li> <li>- AMD (APU FM2+A6) Linea 7000 o superior</li> </ul>	Especificar
Número de modelo:	Especificar
Velocidad:	Especificar



Integrado al motherboard : No.		
<b>Bus</b>		
El bus de datos del motherboard deberá ser de arquitectura PCI / PCI Express.		
<b>Memoria RAM</b>		
Tipo: DDR3 – 1600 MHz o superior.		Especificar
Provisión mínimo: 4Gb.		Especificar
Ampliación: mínimo hasta 8 GB Sin reemplazo de la memoria provista.		Especificar
<b>Disco rígido interno</b>		
Cantidad: 1 (uno)		
Capacidad : Mínimo 500 GB		Especificar
Velocidad de rotación: 7.200 rpm.		Especificar
Interfaz: Serial ATA (SATA III) 6 Gb/s o superior, con compatibilidad disco/motherboard		Especificar
<b>Controlador de Video</b>		
Controladora de vídeo SVGA con acceso a 256 MB RAM como mínimo, arquitectura PCI-E o superior.		
El controlador de video deberá poseer compatibilidad con DirectX 11.		Especificar
<b>Interfaces integradas en la placa madre</b>		



Cuatro (4) puertos USB 3.0	Especificar
Un puerto HDMI	
Interface de red (LAN) integrada RJ45.	
Dispositivo de Red (compatible ETAP PQR-010)	
Capacidad para conectarse a una red local (LAN) tipo Ethernet/IEEE 802.3 o Fast Ethernet/IEEE 802.3u y IEEE 802.3ab autoswitchable.	Especificar
Soporte de medio físico 10 Base-T/100 Base-TX/1000 Base-TX (2 pares UTP categoría 5).	Especificar
Se suministrarán los drivers correspondientes para su correcto funcionamiento bajo los sistemas operativos Windows 7 y versiones superiores	Especificar
Dispositivo de Red WIFI (compatible ETAP PQR-010)	
Capacidad para conectarse a una red inalámbrica local (WLAN) tipo Ethernet/IEEE 802.11 b/g/n	Especificar
Se suministrarán los drivers correspondientes para su correcto funcionamiento bajo los sistemas operativos Windows 7 y versiones superiores	Especificar
Teclado	
Modelo o Número de Parte:	Especificar
Teclado expandido Latinoamericano o Español de por lo menos 84/85 teclas con interface tipo PS/2 o USB, (de construcción rígida.)	Especificar



La inclinación del plano del teclado deberá ser regulable a fin de permitir más de una posición de trabajo. El mecanismo deberá estar integrado a la parte inferior del teclado y de características mecánicas que aseguren su durabilidad.	Especificar
Deberá poseer dispositivos antideslizantes.	Especificar
El material de construcción del teclado deberá ser de calidad tal que soporte uso intensivo.	Especificar
<b>Mouse óptico</b>	
Mouse óptico de dos o tres botones y scrool wheel, con interface tipo USB compatible con los sistemas operativos Windows 7 y versiones superiores	Especificar
<b>Monitor LED</b>	
Modelo:	
Monitor de 18.5" o superior, con una resolución mínima de 1360 x 768 no interlaceado.  Tiempo de Respuesta: no mayor a 5 ms  Relación de Aspecto widescreen (16:9 o 16:10)	Especificar
Cantidad de Colores: Mínimo 16 millones	Especificar
Relación de contraste mínimo: 1000:1 (típico)	Especificar
Controles de: brillo, contraste y amplitud que permitan siempre tener como área visual el total de la pantalla.	Especificar
Angulo de visión: no menor a 160° Horizontal / 160° Vertical	
Brillo: no inferior a 250 cd/m <sup>2</sup>	



Conector: SVGA (D-sub 15) y/o DVI y/o HDMI	Especificar
Certificación: Deberá cumplir con la norma ISO 13406-2 – Clase I (es decir cero (0) pixeles fallados de cualquier tipo).	Especificar
<b>Sistema Operativo</b>	
Se proveerá un sistema operativo Windows 7 Professional 64 bit o posterior con funciones equivalentes o superiores, con manuales originales en castellano y con su correspondiente licencia de uso emitida por la empresa Microsoft. El mismo deberá estar preinstalado. Se deberán proveer el o los CD-ROM de instalación y/o recuperación y/o software de recuperación preinstalado que permita restaurar la instalación original del Sistema Operativo y configuración inicial del equipo	
Los componentes incluidos en el bien del presente Renglón deberán ser compatibles con los sistemas Windows 7 Professional y superiores.	Especificar
<b>Drivers / Controladores (/ Cables)</b>	
Con el equipo se deberán proveer los drivers/controladores y cables necesarios para el correcto funcionamiento del equipo bajo sistema operativo Windows 7 Professional posteriores.	Especificar

#### ETPRTERM – IMPRESORA TERMICA

#### GLOSARIO

En el presente Renglón, los siguientes términos serán interpretados de la manera



que se indica a continuación:

<b>Bien</b>	Es la impresora que el Oferente debe suministrar a la Jurisdicción adquirente en caso de resultar adjudicada su Oferta
<b>Empresa Fabricante</b>	Es la Empresa que fabrica y ensambla los equipos ofrecidos, propietaria de “marca de fábrica”
<b>Equipo equipamiento</b>	/ Es la impresora.
<b>DPSIT</b>	Dirección Provincial de Sistemas de Información y Tecnologías
<i>Marca de fábrica</i>	Es el distintivo o señal que el Fabricante pone a los productos de su empresa, y cuyo uso le pertenece exclusivamente.
<i>Oferente</i>	Es la Persona física o jurídica que presenta Oferta.
<b>Oferta</b>	Es la propuesta de los bienes que se presentan en el acto licitatorio con arreglo a las prescripciones del Pliego de Bases y Condiciones.
<b>Organismo Contratante Comprador</b>	/ Es la Jurisdicción que adquiere los bienes.
<b>Proveedor</b>	Es la Persona física o jurídica adjudicataria que haya perfeccionado el contrato.

#### CONDICIONES PARTICULARES ESPECÍFICAS

##### A - Marca de Fábrica

- Los bienes ofrecidos deberán poseer una única marca de fábrica, siendo la empresa fabricante propietaria de dicha marca, debiendo acreditarse en



	forma fehaciente tal situación.
•	La marca de fábrica de los bienes deberá pertenecer a empresas reconocidas como sociedades comerciales en la República Argentina de acuerdo a la Ley n° 19.550, las cuales podrán ser empresas subsidiarias o controladas o pertenecientes al grupo económico dueño de la marca de fábrica, contando como mínimo con 5 años de radicación en el país.
<b>B - Respecto de los bienes ofertados</b>	
•	<i>Cumplimiento de Norma ISO 14001</i>
	La empresa fabricante del bien ofertado deberá cumplir con la norma ISO 14001 desarrollada por la International Standards Organization. Deberá presentar conjuntamente con la Oferta copia autenticada de la certificación vigente y expedida a favor del fabricante del equipo.
•	<p>El bien ofertado deberá estar en producción al momento de la apertura de Ofertas.</p> <p>Si se dejara de comercializar el bien durante el período entre la presentación de la Oferta y el perfeccionamiento del contrato, la empresa adjudicataria deberá reemplazarlo por el comercializado, el que deberá poseer características técnicas iguales o superiores al ofertado.</p> <p>Ese reemplazo deberá ser previamente autorizado por la Dirección Provincial de Sistemas de Información y Tecnologías.</p> <p>La DPSIT podrá autorizar los cambios en razón de avances tecnológicos que se produjeran en cualquiera de las partes o componentes del equipamiento durante el período de aprovisionamiento o como consecuencia de proveer un nuevo equipo según lo establecido por las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: <b>Defectos de Origen - Vicios de Fabricación – Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía</b> –, siempre que</p>



	dichos avances tecnológicos no modifiquen el objetivo por el que fue adquirido el bien y mantengan o mejoren la prestación del equipamiento.
•	La identificación de marca, modelo y número de serie del equipo deberán ser inviolables, es decir, de calidad tal que imposibilite su remoción y que no pueda ser adulterado, en ambos casos, sin dejar evidencias.
•	El bien ofertado deberá cumplir con las especificaciones técnicas básicas, será nuevo, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso a que el Comprador será el primer usuario del bien desde su fabricación).
•	El oferente deberá garantizar que no existirán limitaciones para que la Superintendencia de Entidades Financieras y Cambiarias tenga acceso a toda documentación técnica relacionada y a la realización de auditorías periódicas en las instalaciones del proveedor.
<b>C - Respecto a la presentación de Ofertas</b>	
•	La Oferta deberá ser presentada por escrito respetando el orden impuesto en las <b>“Especificaciones Técnicas Básicas”</b> , describiendo técnicamente cada uno de los puntos solicitados (leyenda “Especificar”), en forma clara, detallada, precisa y sin ambigüedades. No se admitirá ni se considerará como especificación, descripción o identificación del bien ofrecido leyendas “según pliego” o expresiones de índole similar o referencias a folletos adjuntos.
•	El Oferente deberá integrar a su Oferta la <b>“Planilla de Precios de Lista de Consumibles”</b> . Su no presentación no será subsanable y la Oferta <b>será desestimada</b> .  Los consumibles incluidos en la mencionada planilla deberán ser de la misma marca que aquellos a ser provistos en el equipo original.  El presente llamado a licitación NO TIENE POR OBJETO la provisión de



	<p>los cartuchos indicados como “Consumibles”.</p> <p>Los precios de lista solicitados, deberán ser cotizados en PESOS si son de fabricación nacional. Si son importados podrán cotizarse en DOLARES Estadounidenses, en ambos casos con IVA incluido.</p>
•	<p>Se deberán indicar en la Oferta los consumibles que requiere la impresora para su correcto funcionamiento.</p> <p>Se excluye explícitamente el papel.</p> <p>En las “<b>Especificaciones Técnicas Básicas</b>” se han establecido consumibles considerados en la generalidad de las impresoras láser, pero el Oferente deberá incluir cualquier otro consumible que considere necesario para lograr el objetivo indicado previamente.</p> <p>La estructura a seguir para la descripción de dichos consumibles debe ser según el orden interpuesto en el Punto “Consumible 4 – Otros” de las mencionadas especificaciones.</p> <p>Los consumibles incluidos en las “<b>Especificaciones Técnicas Básicas</b>” y en la “<b>Planilla de Precios de Lista de Consumibles</b>” deberán ser coincidentes.</p>
•	<p>Se deberá adjuntar toda la documentación indicada y establecida en las “<b>Condiciones Particulares Específicas</b>” y las “<b>Especificaciones Técnicas Básicas</b>”.</p>
•	<p>Se podrá, a los fines de lograr una mejor comprensión de las especificaciones consignadas, incluir folletos técnicos (o información impresa proveniente del sitio oficial de la empresa fabricante) del equipo, pudiendo ser presentados en idioma español o en idioma inglés. Se deja establecido que los folletos adjuntos no forman parte de la Oferta.</p>
<b>D - Respecto a la Evaluación de Ofertas</b>	



- Evaluación de la documentación presentada
  - Se evaluará que se haya presentado la documentación requerida en las “**Condiciones Particulares Específicas**” y las “**Especificaciones Técnicas Básicas**”. De existir faltantes, la Oferta será declarada “**No admisible técnicamente**”.
  
  - Si se detectara en la Oferta presentada:
    - que algún consumible no fue incluido,
    - que algún consumible fue incluido sin el detalle solicitado en el Punto 9 del Punto “**C – Respecto a la presentación de Ofertas**”,
    - que algún consumible indicado en las “**Especificaciones Técnicas Básicas**” no se hallare incluido en la “**Planilla de Precios de Lista de Consumibles**”,
    - que no se hubiera indicado la moneda de cotización de algún consumible en la “**Planilla de Precios de Lista de Consumibles**”,esto implicará que, para el presente Renglón, la Oferta **será desestimada**.
  
  - Se verificará que el bien ofrecido cumpla con las “**Condiciones Particulares Específicas**” y las “**Especificaciones Técnicas Básicas**”. En caso que no cumpla, la Oferta será declarada “**No admisible técnicamente**”.
  
  - El comitente podrá solicitar aclaraciones, a través de notificación



fehaciente, donde se establecerá el plazo otorgado para dar respuesta.

#### **E – Respecto a la ponderación económica**

- Con el fin de establecer una metodología para la adquisición del tipo de impresora que se requiere en el presente Renglón, se ha optado por realizar una ponderación económica basado en un análisis sobre los costos generales que impactan sobre el uso de los equipos y que encontrándose algunos en un segundo plano afectan a mediano plazo, el costo final del dispositivo.

#### **Obtención del Costo Teórico de impresión por Hoja**

Se establece la siguiente metodología para calcular el “Costo Teórico de Impresión por Hoja”(CTI<sub>x</sub>H):

- Se convertirán, de corresponder, los precios unitarios de cada consumible consignados en la “**Planilla de Precios de Lista de Consumibles**” a moneda de curso legal, tomando el tipo de cambio vendedor del Banco de la Nación Argentina del Dólar Estadounidense al día de apertura de Ofertas.
- Se calculará el costo teórico de impresión por hoja tomando en cuenta:
  1. Precio unitario del equipo ofrecido, según lo indicado en la “**Planilla de Cotización**” (PU).
  2. Precio de cada consumible en moneda de curso legal, obtenido en el Punto 1 (PC\$)
  3. Cantidad de consumibles necesarios para imprimir mensualmente el 10% de lo solicitado en el Punto “Ciclo mensual de impresión **Mínimo**” de las “**Especificaciones**”



**Técnicas Básicas**” para el período de tiempo indicado en el Punto **“H – Garantía de los bienes”**(CantC).

4. La fórmula general se define:
5. Cálculo de Cantidad de Hojas a imprimir:

$$\text{Cant}_H = 0.10 * \text{CMI} * \text{GM}$$

Donde Cant<sub>H</sub> es la cantidad de hojas estimadas a imprimir.

CMI es el “Ciclo mensual de impresión: **Mínimo**” requerido en las **“Especificaciones Técnicas Básicas”**

GM es la cantidad de meses especificadas en **“H – Garantía de los bienes”** en las **“Condiciones Particulares Específicas”**.

6. Cálculo de Cantidad de Consumibles:

$$\text{CantC}_{(n)} = \text{Cant}_H / R_{(n)}$$

Donde CantC<sub>(n)</sub> es la cantidad de “Consumible n” necesaria para imprimir la cantidad de hojas calculada en el Punto 2.4. a. anterior.

Cant<sub>H</sub> es la cantidad de hojas estimadas a imprimir (calculada en el Punto 2.4. a. anterior).

R<sub>(n)</sub> es el “Rendimiento” declarado en las **“Especificaciones Técnicas Básicas”** para el “Consumible n”.

7. Cálculo del **“Costo Teórico de Impresión por Hoja”**

$$\text{CTI}xH = ( \text{PU} + (\text{CantC}_{(1)} * \text{PC}_{(1)}\$) + \dots + (\text{CantC}_{(n)} * \text{PC}_{(n)}\$) ) / \text{Cant}_H$$

Donde CTI<sub>xH</sub> es el Costo Teórico de Impresión por Hoja



	<p><u>PU</u> es el Precio unitario del equipo.</p> <p><u>PC<sub>(n)</sub>\$</u> es el Precio del “Consumible n” en Pesos, obtenido en el Punto 1.</p> <p><u>Cant_H</u> es la cantidad de hojas estimadas a imprimir calculada en el Punto 2.4. a. anterior.</p> <p><u>CantC<sub>(n)</sub></u> es la cantidad de “Consumible n” necesarios para imprimir la cantidad de hojas Cant_H (CantC<sub>(n)</sub> ha sido calculado en el Punto 2.4. b. anterior).</p> <p>Este valor se calculará con la cantidad de decimales que resulten necesarios para una adecuada evaluación de las Ofertas.</p> <ul style="list-style-type: none"> <li>• En los casos que se hubieran especificado dos alternativas en el consumible indicado como toner, a saber “Toner de capacidad estándar” y “Toner de alta capacidad”, se calcularán dos alternativas para el mismo equipo.</li> </ul>
<p><b>F - Preadjudicación</b></p>	
<ul style="list-style-type: none"> <li>•</li> </ul>	<ul style="list-style-type: none"> <li>• La preadjudicación recaerá en la propuesta más conveniente, de acuerdo al siguiente procedimiento:             <ol style="list-style-type: none"> <li>1. Se considerarán técnicamente admisibles, aquellas Ofertas que hayan cumplido los requerimientos indicados en el Punto “D – <b>Respecto a la Evaluación de Ofertas</b>”.</li> <li>2. Se preadjudicará a la propuesta de menor costo teórico de impresión por hoja según lo establecido en el Punto “E – <b>Respecto a la ponderación económica</b>”. En caso de</li> </ol> </li> </ul>



	<p>igualdad de costos teóricos de impresión por hoja, la preadjudicación recaerá en aquella propuesta de menor precio unitario del equipo.</p>
<b>G - Recepción de bienes</b>	
•	El Adjudicatario deberá proveer los manuales técnicos y de usuario originales (no siendo permitido la presentación de fotocopias) correspondientes a los bienes entregados, preferentemente en castellano o en su defecto en inglés.
•	El Adjudicatario deberá proveer los cables a la red eléctrica y a la PC.
<b>H - Garantía de los bienes</b>	
•	<ul style="list-style-type: none"> <li>• Garantía.           <ol style="list-style-type: none"> <li>1. Los bienes suministrados tendrán una garantía de la empresa fabricante por un término de 36 meses.</li> <li>2. Garantía de buen funcionamiento:               <ol style="list-style-type: none"> <li>1. En el caso del hardware, la “Garantía de buen funcionamiento” abarcará todo el período indicado en el Punto 1.1 y deberá cumplir los siguientes requisitos:                   <ol style="list-style-type: none"> <li>1. La presente garantía incluirá el servicio de reparación por personal calificado con la provisión y el reemplazo de las partes que se encuentren defectuosas por repuestos originales. Los elementos reemplazantes deberán ser de las mismas características o</li> </ol> </li> </ol> </li> </ol> </li> </ul>



en su defecto equivalentes en su rendimiento según las pautas de calidad establecidas por el fabricante del bien entregado y las exigidas en las “Especificaciones Técnicas Básicas”. Deberá presentarse, en caso de ser requerido, la documentación que respalde lo previamente expuesto.

2. A efectos de cumplimentar con el servicio de garantía, el equipamiento se centralizará en una dependencia del Organismo Contratante, la cual podrá ser establecida dentro de la ciudad de La Plata y su área de influencia y la Ciudad Autónoma de Buenos Aires, donde la empresa fabricante deberá repararlo o retirarlo para su reparación. Los gastos de traslado desde y hacia esa dependencia estarán a cargo exclusivo del proveedor. (Se define al área de influencia de la ciudad de La Plata a los partidos de La Plata, Berisso y Ensenada).
3. La reparación de los bienes deberá ser ejecutada a satisfacción del Comprador. El tiempo de respuesta entre el pedido de reparación y el inicio de la misma no podrá superar las 24 hs. El tiempo máximo de reparación será de siete (7) días. El horario disponible para reclamos deberá ser de 9.00 hs. a 18 hs.



Se define “El tiempo de respuesta entre el pedido de reparación y el inicio de la misma” al tiempo máximo que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y la presencia de personal técnico idóneo con el fin de determinar la avería en el equipo afectado.

Se define “El tiempo máximo de reparación” al lapso que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y el momento en que el organismo recepciona y verifica el buen funcionamiento del bien afectado.

4. La cantidad de días de indisponibilidad, según se define en las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: **Defectos de Origen - Vicios de Fabricación - Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía** –, se establece en sesenta (60) días.

#### I – Respecto del Precio de Consumibles

- El Oferente deberá integrar a su oferta, el compromiso de la empresa fabricante de los equipos a mantener como valores máximos, los importes cotizados en la “Planilla de Precios de Lista de Consumibles”.por el período de vigencia de la Garantía y su disponibilidad.
- El Oferente deberá garantizar a los Organismos Contratantes, la provisión de consumibles que sean requeridos, durante el período de garantía del



	equipo adquirido y según la cotización efectuada en el presente llamado, <b><u>“Planilla de Precios de Lista de Consumibles”</u></b> .
•	En la <b>“Planilla de Precios de Lista de Consumibles”</b> se deberá indicar el código de parte de cada insumo cotizado.

<b>ESPECIFICACIONES TECNICAS BASICAS</b>	
Marca del Equipo:	
Modelo del Equipo:	
Resolución: en calidad optimizada mínimo 600 dpi	Especificar
Memoria: mínimo 256 Mb. Buffer de datos: recepción a 45 bytes o 4 KB, seleccionable; definido por el usuario: 12KB; macro: 2KB - Gráficos NV: 256KB; Usuario NV: 1KB - Normas EMI: FCC/ICES-003 Clase A.	Especificar
Velocidad de impresión: mínimo 11,8"/Seg (300 mm) para grafico y textos 2,4"/seg para código de barras	Especificar
Manejo de papel: • Deberá tener la capacidad de admitir al menos dos Fuentes de entrada. • Fuente A: 12x24 • Fuente B:9x17 (incluido espacio horizontal de dos puntos)	Especificar



<ul style="list-style-type: none"> <li>• Capacidad de columnas: 80 mm: 42/56 columnas; modelo de 58mm: 30/40 columnas.</li> <li>• Tamaños de papel: 80 mm: Diámetro de 3,13" +- 0,02" x 3,27" (79,5 +- 0,5 (ancho) x 83 mm), 58mm: Diámetro de 2,26" +- 0,02" x 3,27" (57,5 +- 0,5 (ancho) x 83 mm)</li> <li>• - Espesor Papel: 55 – 80 micrones</li> </ul>	
<p>Buffer de datos: recepción a 45 bytes o 4 KB, seleccionable; definido por el usuario: 12KB; macro: 2KB</p> <p>- Gráficos NV: 256KB; Usuario NV: 1KB</p> <p>- Normas EMI: FCC/ICES-003 Clase A.</p> <p>Juego de caracteres: 95 alfanuméricos, 18 internaciones, 128 x 43 grafico (incluida página definida por el usuario).</p> <p>- Código de barras: UPC-A/E, CODE 39/93/128, EAN8/PDF417, 13, ITF, símbolos CODABAR 2D: QR-CODE, MaxiCode, Composite Symbology, GS1-127, GS1 DataBar Omnidireccional/truncado/limitado/expandido</p>	Especificar
<p>Confiabilidad</p> <ul style="list-style-type: none"> <li>• Tiempo medio entre fallas: 360.000 horas.</li> <li>• Ciclo medio entre fallas: 70.000.000 líneas</li> </ul>	Especificar
<p>Interface USB incorporada + otra selección: RS-232C en serie, IEEE-1284 paralela, USB de alta velocidad, alimentación desde USB, Ethernet 10/100Base-t/TX</p>	Especificar



Con el equipo se deberán proveer los drivers y cables necesarios para el correcto funcionamiento del equipo bajo sistema operativo Windows 7 y posteriores.	Especificar
<b>Consumible 1 – Toner</b>	
Descripción: Toner de capacidad estándar	Si / No
Rendimiento: (Según Norma ISO/IEC 19752 )	Especificar
<b>Consumible 2 – Toner</b>	
Descripción: Toner de alta capacidad	Si / No
Rendimiento: (Según Norma ISO/IEC 19752 )	Especificar
<b>Consumible 3</b>	
Descripción: Kit de Mantenimiento	Si / No
Rendimiento: Recomendación de cambio (Según Norma ISO/IEC 19752 )	Especificar
<b>Consumible 4 – Otros</b>	
Descripción:	Si (Especificar) / No
Rendimiento: Recomendación de cambio (Según Norma ISO/IEC 19752 )	Especificar

### PLANILLA DE PRECIOS DE LISTA DE CONSUMIBLES

Empresa:

325

PLIEG-2017-05863125-GDEBA-DJLIPLYC



Renglón	Descripción	Precio Unitario (Indicar moneda -\$ o U\$S- )
	Impresora en red para Oficina Grande - Láser monocromática	
	Consumible 1 – Toner de capacidad estándar	
	Consumible 2 – Tóner de alta capacidad	
	Consumible 3 – Kit de Mantenimiento	
	Consumible 4 – (Especificar)	
	Consumible.... – (Especificar)	

#### ETPRTLSDPL – IMPRESORA LASER RED DUPLEX

GLOSARIO	
En el presente Renglón, los siguientes términos serán interpretados de la manera que se indica a continuación:	
<b>Bien</b>	Es la impresora que el Oferente debe suministrar a la Jurisdicción adquirente en caso de resultar adjudicada su Oferta
<b>Empresa Fabricante</b>	Es la Empresa que fabrica y ensambla los equipos ofrecidos, propietaria de “marca de fábrica”



<b>Equipo equipamiento</b>	/	Es la impresora.
<b>DPSIT</b>		Dirección Provincial de Sistemas de Información y Tecnologías
<b>Marca de fábrica</b>	<b>de</b>	Es el distintivo o señal que el Fabricante pone a los productos de su empresa, y cuyo uso le pertenece exclusivamente.
<b>Oferente</b>		Es la Persona física o jurídica que presenta Oferta.
<b>Oferta</b>		Es la propuesta de los bienes que se presentan en el acto licitatorio con arreglo a las prescripciones del Pliego de Bases y Condiciones.
<b>Organismo Contratante / Comprador</b>		Es la Jurisdicción que adquiere los bienes.
<b>Proveedor</b>		Es la Persona física o jurídica adjudataria que haya perfeccionado el contrato.

#### CONDICIONES PARTICULARES ESPECÍFICAS

##### A - Marca de Fábrica

- Los bienes ofrecidos deberán poseer una única marca de fábrica, siendo la empresa fabricante propietaria de dicha marca, debiendo acreditarse en forma fehaciente tal situación.
- La marca de fábrica de los bienes deberá pertenecer a empresas reconocidas como sociedades comerciales en la República Argentina de acuerdo a la Ley n° 19.550, las cuales podrán ser empresas subsidiarias o controladas o pertenecientes al grupo económico dueño de la marca de



	fábrica, contando como mínimo con 5 años de radicación en el país.
<b>B - Respetto de los bienes ofertados</b>	
•	<b>Cumplimiento de Norma ISO 14001</b>
	La empresa fabricante del bien ofertado deberá cumplir con la norma ISO 14001 desarrollada por la International Standards Organization. Deberá presentar conjuntamente con la Oferta copia autenticada de la certificación vigente y expedida a favor del fabricante del equipo.
•	<p>El bien ofertado deberá estar en producción al momento de la apertura de Ofertas.</p> <p>Si se dejara de comercializar el bien durante el período entre la presentación de la Oferta y el perfeccionamiento del contrato, la empresa adjudicataria deberá reemplazarlo por el comercializado, el que deberá poseer características técnicas iguales o superiores al ofertado.</p> <p>Ese reemplazo deberá ser previamente autorizado por la Dirección Provincial de Sistemas de Información y Tecnologías.</p> <p>La DPSIT podrá autorizar los cambios en razón de avances tecnológicos que se produjeran en cualquiera de las partes o componentes del equipamiento durante el período de aprovisionamiento o como consecuencia de proveer un nuevo equipo según lo establecido por las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: <b>Defectos de Origen - Vicios de Fabricación – Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía</b> –, siempre que dichos avances tecnológicos no modifiquen el objetivo por el que fue adquirido el bien y mantengan o mejoren la prestación del equipamiento.</p>
•	La identificación de marca, modelo y número de serie del equipo deberán ser inviolables, es decir, de calidad tal que imposibilite su remoción y que



	no pueda ser adulterado, en ambos casos, sin dejar evidencias.
•	El bien ofertado deberá cumplir con las especificaciones técnicas básicas, será nuevo, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso a que el Comprador será el primer usuario del bien desde su fabricación).
•	El oferente deberá garantizar que no existirán limitaciones para que la Superintendencia de Entidades Financieras y Cambiarias tenga acceso a toda documentación técnica relacionada y a la realización de auditorías periódicas en las instalaciones del proveedor.
<b>C - Respecto a la presentación de Ofertas</b>	
•	La Oferta deberá ser presentada por escrito respetando el orden impuesto en las <b>“Especificaciones Técnicas Básicas”</b> , describiendo técnicamente cada uno de los puntos solicitados (leyenda “Especificar”), en forma clara, detallada, precisa y sin ambigüedades. No se admitirá ni se considerará como especificación, descripción o identificación del bien ofrecido leyendas “según pliego” o expresiones de índole similar o referencias a folletos adjuntos.
•	El Oferente deberá integrar a su Oferta la <b>“Planilla de Precios de Lista de Consumibles”</b> . Su no presentación no será subsanable y la Oferta <b>será desestimada</b> .  Los consumibles incluidos en la mencionada planilla deberán ser de la misma marca que aquellos a ser provistos en el equipo original.  El presente llamado a licitación NO TIENE POR OBJETO la provisión de los cartuchos indicados como “Consumibles”.  Los precios de lista solicitados, deberán ser cotizados en PESOS si son de fabricación nacional. Si son importados podrán cotizarse en DOLARES



	Estadounidenses, en ambos casos con IVA incluido.
•	<p>Se deberán indicar en la Oferta los consumibles que requiere la impresora para su correcto funcionamiento.</p> <p>Se excluye explícitamente el papel.</p> <p>En las “<b><u>Especificaciones Técnicas Básicas</u></b>” se han establecido consumibles considerados en la generalidad de las impresoras láser, pero el Oferente deberá incluir cualquier otro consumible que considere necesario para lograr el objetivo indicado previamente.</p> <p>La estructura a seguir para la descripción de dichos consumibles debe ser según el orden interpuesto en el Punto “Consumible 4 – Otros” de las mencionadas especificaciones.</p> <p>Los consumibles incluidos en las “<b><u>Especificaciones Técnicas Básicas</u></b>” y en la “<b><u>Planilla de Precios de Lista de Consumibles</u></b>” deberán ser coincidentes.</p>
•	Se deberá adjuntar toda la documentación indicada y establecida en las “ <b><u>Condiciones Particulares Específicas</u></b> ” y las “ <b><u>Especificaciones Técnicas Básicas</u></b> ”.
•	Se podrá, a los fines de lograr una mejor comprensión de las especificaciones consignadas, incluir folletos técnicos (o información impresa proveniente del sitio oficial de la empresa fabricante) del equipo, pudiendo ser presentados en idioma español o en idioma inglés. Se deja establecido que los folletos adjuntos no forman parte de la Oferta.
<b>D - Respecto a la Evaluación de Ofertas</b>	



• **Evaluación de la documentación presentada**

- Se evaluará que se haya presentado la documentación requerida en las “**Condiciones Particulares Específicas**” y las “**Especificaciones Técnicas Básicas**”. De existir faltantes, la Oferta será declarada “**No admisible técnicamente**”.

- Si se detectara en la Oferta presentada:

- que algún consumible no fue incluido,

- que algún consumible fue incluido sin el detalle solicitado en el Punto 9 del Punto “**C – Respecto a la presentación de Ofertas**”,

- que algún consumible indicado en las “**Especificaciones Técnicas Básicas**” no se hallare incluido en la “**Planilla de Precios de Lista de Consumibles**”,

- que no se hubiera indicado la moneda de cotización de algún consumible en la “**Planilla de Precios de Lista de Consumibles**”,

esto implicará que, para el presente Renglón, la Oferta **será desestimada**.

- Se verificará que el bien ofrecido cumpla con las “**Condiciones Particulares Específicas**” y las “**Especificaciones Técnicas Básicas**”. En caso que no cumpla, la Oferta será declarada “**No admisible técnicamente**”.

- El comitente podrá solicitar aclaraciones, a través de notificación



	fehaciente, donde se establecerá el plazo otorgado para dar respuesta.
<b>E – Respecto a la ponderación económica</b>	
•	<p>Con el fin de establecer una metodología para la adquisición del tipo de impresora que se requiere en el presente Renglón, se ha optado por realizar una ponderación económica basado en un análisis sobre los costos generales que impactan sobre el uso de los equipos y que encontrándose algunos en un segundo plano afectan a mediano plazo, el costo final del dispositivo.</p> <p><b><u>Obtención del Costo Teórico de impresión por Hoja</u></b></p> <p>Se establece la siguiente metodología para calcular el “Costo Teórico de Impresión por Hoja”(CTIxH):</p> <ul style="list-style-type: none"> <li>• Se convertirán, de corresponder, los precios unitarios de cada consumible cosignados en la “<b><u>Planilla de Precios de Lista de Consumibles</u></b>” a moneda de curso legal, tomando el tipo de cambio vendedor del Banco de la Nación Argentina del Dólar Estadounidense al día de apertura de Ofertas.</li> <li>• Se calculará el costo teórico de impresión por hoja tomando en cuenta:             <ol style="list-style-type: none"> <li>1. Precio unitario del equipo ofrecido, según lo indicado en la “<b><u>Planilla de Cotización</u></b>” (PU).</li> <li>2. Precio de cada consumible en moneda de curso legal, obtenido en el Punto 1 (PC\$)</li> <li>3. Cantidad de consumibles necesarios para imprimir mensualmente el 10% de lo solicitado en el Punto “Ciclo mensual de impresión <b>Mínimo</b>” de las “<b><u>Especificaciones</u></b></li> </ol> </li> </ul>



**Técnicas Básicas**” para el período de tiempo indicado en el Punto **“H – Garantía de los bienes”**(CantC).

4. La fórmula general se define:
5. Cálculo de Cantidad de Hojas a imprimir:

$$\text{Cant}_H = 0.10 * \text{CMI} * \text{GM}$$

Donde Cant<sub>H</sub> es la cantidad de hojas estimadas a imprimir.

CMI es el “Ciclo mensual de impresión: **Mínimo**” requerido en las **“Especificaciones Técnicas Básicas”**

GM es la cantidad de meses especificadas en **“H – Garantía de los bienes”** en las **“Condiciones Particulares Específicas”**.

6. Cálculo de Cantidad de Consumibles:

$$\text{CantC}_{(n)} = \text{Cant}_H / R_{(n)}$$

Donde CantC<sub>(n)</sub> es la cantidad de “Consumible n” necesarios para imprimir la cantidad de hojas calculada en el Punto 2.4. a. anterior.

Cant<sub>H</sub> es la cantidad de hojas estimadas a imprimir (calculada en el Punto 2.4. a. anterior).

R<sub>(n)</sub> es el “Rendimiento” declarado en las **“Especificaciones Técnicas Básicas”** para el “Consumible n”.

7. Cálculo del **“Costo Teórico de Impresión por Hoja”**



$$CTixH = ( PU + (CantC_{(1)} * PC_{(1)}\$) + \dots + (CantC_{(n)} * PC_{(n)}\$) ) / Cant\_H$$

Donde CTixH es el Costo Teórico de Impresión por Hoja

PU es el Precio unitario del equipo.

PC<sub>(n)</sub>\$ es el Precio del “Consumible n” en Pesos, obtenido en el Punto 1.

Cant\_H es la cantidad de hojas estimadas a imprimir calculada en el Punto 2.4. a. anterior.

CantC<sub>(n)</sub> es la cantidad de “Consumible n” necesarios para imprimir la cantidad de hojas Cant\_H (CantC<sub>(n)</sub> ha sido calculado en el Punto 2.4. b. anterior).

Este valor se calculará con la cantidad de decimales que resulten necesarios para una adecuada evaluación de las Ofertas.

- En los casos que se hubieran especificado dos alternativas en el consumible indicado como toner, a saber “Toner de capacidad estándar” y “Toner de alta capacidad”, se calcularán dos alternativas para el mismo equipo.

#### F - Preadjudicación

- La preadjudicación recaerá en la propuesta más conveniente, de acuerdo al siguiente procedimiento:
  1. Se considerarán técnicamente admisibles, aquellas Ofertas que hayan cumplido los requerimientos indicados en el



	<p>Punto “D – <b>Respecto a la Evaluación de Ofertas</b>”.</p> <p>2. Se preadjudicará a la propuesta de menor costo teórico de impresión por hoja según lo establecido en el Punto “E – <b>Respecto a la ponderación económica</b>”. En caso de igualdad de costos teóricos de impresión por hoja, la preadjudicación recaerá en aquella propuesta de menor precio unitario del equipo.</p>
<b>G - Recepción de bienes</b>	
•	El Adjudicatario deberá proveer los manuales técnicos y de usuario originales (no siendo permitido la presentación de fotocopias) correspondientes a los bienes entregados, preferentemente en castellano o en su defecto en inglés.
•	El Adjudicatario deberá proveer los cables a la red eléctrica y a la PC.
<b>H - Garantía de los bienes</b>	
•	<ul style="list-style-type: none"> <li>• Garantía.           <ol style="list-style-type: none"> <li>1. Los bienes suministrados tendrán una garantía de la empresa fabricante por un término de 36 meses.</li> <li>2. Garantía de buen funcionamiento:               <ol style="list-style-type: none"> <li>1. En el caso del hardware, la “Garantía de buen funcionamiento” abarcará todo el período indicado en el Punto 1.1 y deberá cumplir los siguientes requisitos:                   <ol style="list-style-type: none"> <li>1. La presente garantía incluirá el servicio de reparación por personal calificado con la</li> </ol> </li> </ol> </li> </ol> </li> </ul>



	<p>provisión y el reemplazo de las partes que se encuentren defectuosas por repuestos originales. Los elementos reemplazantes deberán ser de las mismas características o en su defecto equivalentes en su rendimiento según las pautas de calidad establecidas por el fabricante del bien entregado y las exigidas en las “Especificaciones Técnicas Básicas”. Deberá presentarse, en caso de ser requerido, la documentación que respalde lo previamente expuesto.</p> <p>2. A efectos de cumplimentar con el servicio de garantía, el equipamiento se centralizará en una dependencia del Organismo Contratante, la cual podrá ser establecida dentro de la ciudad de La Plata y su área de influencia y la Ciudad Autónoma de Buenos Aires, donde la empresa fabricante deberá repararlo o retirarlo para su reparación. Los gastos de traslado desde y hacia esa dependencia estarán a cargo exclusivo del proveedor. (Se define al área de influencia de la ciudad de La Plata a los partidos de La Plata, Berisso y Ensenada).</p> <p>3. La reparación de los bienes deberá ser ejecutada a satisfacción del Comprador. El tiempo de respuesta entre el pedido de reparación y el inicio de la misma no podrá superar las 24 hs. El tiempo máximo de</p>
--	---



reparación será de siete (7) días. El horario disponible para reclamos deberá ser de 9.00 hs. a 18 hs.

Se define “El tiempo de respuesta entre el pedido de reparación y el inicio de la misma” al tiempo máximo que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y la presencia de personal técnico idóneo con el fin de determinar la avería en el equipo afectado.

Se define “El tiempo máximo de reparación” al lapso que transcurre entre el momento en que se notifica al proveedor el mal funcionamiento de un equipo y el momento en que el organismo recepciona y verifica el buen funcionamiento del bien afectado.

4. La cantidad de días de indisponibilidad, según se define en las Condiciones Particulares del Pliego de Bases y Condiciones – Punto: **Defectos de Origen - Vicios de Fabricación - Extensión - Reemplazo de elementos - Garantía - Afianzamiento de Garantía** –, se establece en sesenta (60) días.

#### I – Respetto del Precio de Consumibles

- El Oferente deberá integrar a su oferta, el compromiso de la empresa fabricante de los equipos a mantener como valores máximos, los importes cotizados en la “Planilla de Precios de Lista de Consumibles”.por el



	período de vigencia de la Garantía y su disponibilidad.
•	El Oferente deberá garantizar a los Organismos Contratantes, la provisión de consumibles que sean requeridos, durante el período de garantía del equipo adquirido y según la cotización efectuada en el presente llamado, <b><u>“Planilla de Precios de Lista de Consumibles”</u></b> .
•	En la <b>“Planilla de Precios de Lista de Consumibles”</b> se deberá indicar el código de parte de cada insumo cotizado.

<b>ESPECIFICACIONES TECNICAS BASICAS</b>	
Marca del Equipo:	
Modelo del Equipo:	
Resolución: en calidad optimizada mínimo 1200 dpi	Especificar
Memoria: mínimo 128 Mb. , expandible a 512 Mb.	Especificar
Velocidad de impresión: mínimo 50 páginas por minuto (tamaño Carta o A4)	Especificar
Manejo de papel:	Especificar
<ul style="list-style-type: none"> <li>• Deberá tener la capacidad de admitir de 600 hojas en un mínimo de 2 bandejas de entradas.</li> <li>• Tamaño de papel soportados: Legal, carta, A4.</li> </ul>	
Lenguaje: PCL 6 (o emulación) y PostScript Nivel 3 (o emulación) .	Especificar
Ciclo mensual de impresión:	Especificar



<ul style="list-style-type: none"> <li>Mínimo: 200.000 páginas por mes (EXCLUYENTE)</li> <li>Máximo: 300.000 páginas por mes (EXCLUYENTE)</li> </ul>	
Interface: USB 2.0 y/o LAN(RJ45) y/o WIFI	Especificar
Con el equipo se deberán proveer los drivers y cables necesarios para el correcto funcionamiento del equipo bajo sistema operativo Windows 7 y posteriores.	Especificar
<b>Consumible 1 – Toner</b>	
Descripción: Toner de capacidad estándar	Si / No
Rendimiento: (Según Norma ISO/IEC 19752 )	Especificar
<b>Consumible 2 – Toner</b>	
Descripción: Toner de alta capacidad	Si / No
Rendimiento: (Según Norma ISO/IEC 19752 )	Especificar
<b>Consumible 3</b>	
Descripción: Kit de Mantenimiento	Si / No
Rendimiento: Recomendación de cambio (Según Norma ISO/IEC 19752 )	Especificar
<b>Consumible 4 – Otros</b>	
Descripción:	Si (Especificar) / No
Rendimiento: Recomendación de cambio (Según Norma ISO/IEC 19752 )	Especificar



## PLANILLA DE PRECIOS DE LISTA DE CONSUMIBLES

### Empresa:

Renglón	Descripción	Precio Unitario (Indicar moneda -\$ o US\$- )
	Impresora en red para Oficina Grande - Láser monocromática	
	Consumible 1 – Toner de capacidad estándar	
	Consumible 2 – Toner de alta capacidad	
	Consumible 3 – Kit de Mantenimiento	
	Consumible 4 – (Especificar)	
	Consumible ..... – (Especificar)	

### **ETRDRUSB – LECTOR TARJETAS RFID USB**



- Lee tarjetas y llaveros RFID de 125 khz., con salida USB
- Tamaño: 55 x 75 mm., profundidad 30 mm.
- Alimentación: 9 a 12 VCA o VCC, mínimo 50 ma.
- Temperatura de Operación: -40 a +85 °C.
- Rango de lectura: Max. 10 cm.
- Frecuencia de operación: 125 Khz.
- Codificación: Manchester 64 bits.
- Salida: USB.

#### **ETFWCENTRAL: Firewall Perimetral tipo UTM para sitio central**

*Unidades:* 2 (1 cluster de dos equipos)

Adquisición de un sistema de seguridad informática perimetral que sea 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 en el presente documento.

El mismo será posicionado como punto central de convergencia de VPNs de múltiples sitios y usuarios, y a su vez debe tener la capacidad de inspección de todo el tráfico que reciba por las mismas.

#### **Características del dispositivo**

341



- El dispositivo debe ser un equipo de propósito específico.
- Basado en tecnología ASIC y que sea capaz de brindar una solución de “Complete Content Protection”. 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 de forma local ciertas consultas de acuerdo a la configuración del administrador.
- El equipo de seguridad 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.
- Debe contar con fuentes redundantes internas o externas para asegurar el funcionamiento ante posibles cortes de energía.
- La solución proporcionada debe contar con un formato rackeable de hasta 2 unidades de rack.

## Firewall

- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.



- Por granularidad y seguridad, 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.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia 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),
- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.



- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
- El equipo 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.
- El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN
- La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.
- La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada
- La solución será capaz de integrar los servicios dentro de las 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
- La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo
- La solución 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
- El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.
- El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS



- La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o específica
- La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
- El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados
- El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico
- Tendrá la capacidad de hacer escaneo a profundidad de tráfico 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 cuál de 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)



- Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento. En este modo, 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
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
- La solución podrá habilitar políticas de ruteo en IPv6
- La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6
- La solución 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 explícito
- Deberá ser capaz de integrar políticas con proxy explícito en IPv6
- La solución podrá restringir direcciones IPv6 en modo proxy explícito
- 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
- La solución 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 para el trafico en IPv6
- El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6
- La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface
- La solución deberá contar 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.
- Se debe soportar 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.
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSeC client-to-site.
- La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)



- En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de 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. En este modo, 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 algún 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, entendiéndose como 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 que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autenticación nuevamente.

### **Traffic Shapping / QoS**

- Capacidad de poder asignar parámetros de traffic shapping
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente
- Capacidad de poder definir ancho de banda garantizado
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo)
- 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 sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”
- Capacidad de 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.
- Debe ser posible 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. Esto significa que podrán 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.
- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
  - 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 “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo 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 appliance, 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 incluir 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” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas)

### AntiSpam

- La capacidad antispam incluida deberá ser capaz de 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 incluida 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 listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
- 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
- En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.



### Filtrado de URLs (URL Filtering)

- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
- 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, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo 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, bloqueando cualquier tipo de contenido no Educativo.
- 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 la página completa.
  2. Modo Proxy: La pagina 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.
- La funcionalidad de reputación busca que, al acceder a paginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una pagina de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red.



- El sistema de filtrado de URLs debe incluir la 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 código en la configuración de filtrado de URLs del equipo para poder habilitar únicamente 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" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones 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 de 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. También podrá definirse el bloqueo 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:
  - 1. 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 periódica por el fabricante.



- 2. 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.
- La funcionalidad 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 la detección de una posible fuga de información deben poder aplicarse el menos 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, la solución 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:
  1. Filtrado por tipo de archivo
  2. Filtrado por nombre de archivo
  3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.



4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.

5. 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**

- Lo solución debe soportar la capacidad de 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.
- Las 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 poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes 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

#### **Controlador Inalámbrico (Wireless Controller)**

- El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless
- En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación.
- Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection.
- El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs.
- Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.
- La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el tráfico wireless para detectar y reportar posibles intentos de intrusión.



- Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente.
- El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta.
- El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off.
- Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred.
- El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz grafica (GUI)
- El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota.
- El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión.
- El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricas dentro del mismo segmento de red.
- El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad,
- El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC



- El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletás, Laptops, PCs (tanto en Windows como en Linux)
- El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.

### **Filtrado de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea**

- Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).
- El dispositivo deberá 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.
- En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.
- La solución debe contar con un ALG (Application Layer Gateway) de SIP
- Debe poder hacerse 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 tráfico SSH en modo proxy explícito
- La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explícito 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**

- La solución 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 la 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 tráfico 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
- Alta Disponibilidad en modo 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 y que forme 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. Este puerto debe estar 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 especificar 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 bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2
- Soporte de SNMP versión 3
- Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
- Soporte para 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 cuando ocurra 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 grafica.



- Contar con facilidades de administración a través de la interfaz grafica como listas de edición a través de click derecho.
- Contar con facilidades de administración a través de la interfaz grafica como 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.
- Contar con herramientas graficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

### Virtualización

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”
- La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus
- Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.
- 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.
- Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el tráfico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.

### **Análisis de Seguridad y Almacenamiento de Logs en la Nube**

- La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función.
- Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legítimo o ilegítimo, por medio de técnicas de Caja de Arena o Sandboxing.
- Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse.
- Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz.
- Permitir Monitoreo y alertas en tiempo real.
- Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis.
- Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.

### **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

### **3.- Licenciamiento y actualizaciones**

#### **\* Tamaño de licencia**

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.

#### **\* Vigencia de licencia de actualización**

La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos 3 años.

### **4.- Desempeño / Conectividad**

El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad



Numero de Interfaces Requeridas	16x 1GE SFP, 16x GE RJ45, 4x 10GB SFP+, 2x 1GE RJ45 para Management.
Throughput de Firewall (con paquetes de 1518/512/64 byte)	72 Gbps/72 Gbps/56 Gbps
Latencia de firewall (con paquetes de 64 byte)	3 $\mu$ s
Paquetes por Segundo procesados por el Firewall	78 Mpps
Throughput de VPN IPSec (con paquetes de 512 byte)	48 Gbps
Throughput de NGFW	2,4 Gbps
Throughput de IPS (HTTP/Enterprise Mix)	11 Gbps / 6,8 Gbps
Throughput de Inspección SSL	6 Gbps
Políticas de Firewall admitidas	100.000
Tuneles gateway to gateway	20.000
Tuneles client to gateway	50.000
Tuneles SSL	10.000
Throughput VPN SSL	3,6 Gbps
Sesiones Concurrentes	11 Millones
Nuevas sesiones / segundo	290.000
Storage (SSD)	1.



## **5 - Sistema de gestión centralizado**

Contar con un sistema de administración centralizada capaz de operar, reportar y mantener remotamente múltiples dispositivos de seguridad desde una única plataforma. El sistema deberá facilitar la tarea de gestión en entornos masivos multiplataforma.

### **1. Funcionalidades y Características del Sistema:**

- Sistema de gerenciamiento (consola de administración) centralizado que realiza aprovisionamiento basado en políticas, configuración de dispositivos, gerenciamiento de actualizaciones, monitoreo y control de dispositivos de seguridad. Entre sus tareas se define:
  - Administración remota de múltiples dispositivos
  - Opción de política independiente o única
  - Definición de una única base de objetos dinámicos
  - Respaldo múltiple de configuraciones.
  - Definición de zonas o entornos virtuales
  - Manejo de actualizaciones y servicios
  - Scripting
  - Tareas calendarizadas
  - Reportes
  - Monitoreo

### **Requerimiento de sistema**



- Centralización de Configuración y monitoreo de todos los dispositivos de seguridad, (mínimamente firewalls o firewalls UTM) así como todas sus funciones de protección de red
- Por seguridad y eficiencia, debe ser un “appliance” virtual o físico de propósito específico para el gerenciamiento de la seguridad. No se aceptan plataformas basadas en sistemas operativos genéricos y/o hardware genérico.
- Deberá permitir la administración de dispositivos “virtuales” que residen en una misma unidad física. Estos equipos virtuales pueden ser administrados como un dispositivo completamente independiente dentro de la consola, con su propia configuración y administración. Esta capacidad permite consolidar en el número menor posible de consolas, preferentemente una, la administración de las diversas funcionalidades de protección completa de contenido.
- Debe poder correr en plataformas de virtualización como VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM y Amazon Web Services (AWS)

### **Funcionalidades**

- Creación, almacenamiento e implementación automatizada de configuraciones de dispositivos.
- Permitir 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 deben ser cifradas (Encriptadas)
- La interface de administración es 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 una mejor flexibilidad y control. Esta funcionalidad permite la automatización de tareas operativas, cuya implementación puede ser de forma masiva, con tiempos de aplicación mínimos a los dispositivos administrados
- Se debe poder realizar automatización calendarizada de respaldos de la configuración y las bitácoras.
- Se debe poder realizar operaciones sobre grupos de dispositivos, y añadir/cambiar/borrar dispositivos de esos grupos.
- Permitir el hospedaje local de actualizaciones de firmas de AV / IPS y filtrado de contenido web y Antispam, de los firewalls de nueva generación. Esto permite el almacenamiento de forma local de las bases de datos de protección AV e IPS, además de Filtrado de Contenido y Anti-SPAM, con la finalidad de disminuir el tráfico de consultas de actualizaciones a Internet a lo mínimo, evitando el consumo innecesario de ancho de banda, permitiendo la utilización de este para los fines requeridos por los usuarios de red.
- Capacidad de crear, exportar y almacenar versiones de configuración de los dispositivos administrados, antes de aplicar cambios a un dispositivo. De esta forma, se disminuye la posibilidad de cometer un error no intencional al modificar una política y permite regresar a una configuración en un estado operacional después de haber aplicado una implementación con resultados no esperados.
- Capacidad de ejecución de scripts para automatización en el aprovisionamiento de dispositivos, políticas, etc.
- La solución deberá proveer opciones de integración mediante APIs (XML, JSON) para la definición y personalización de entornos anexos.



- Posibilidad de 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 administrados por la consola, reduciendo tiempos de operación y administración del personal que administra los equipos de seguridad.
- La consola de administración permite 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 en esquema de comunidades
- Debe soportar al menos 20 modelos diferentes de dispositivos o firewalls.
- Cuando se requiera, deberá poder gestionar de forma independiente o integrada puntos de acceso inalámbricos asociados a los controladores gestionados.

### ***Monitoreo y Reportería***

- Deberá incluir un subsistema de Monitoreo en Tiempo-Real . Esto permite al equipo de monitoreo y administración obtener el estado actual de la infraestructura de dispositivos administrados, y permitir actuar proactivamente a un evento de seguridad y operación de los dispositivos de seguridad administrados.
- Deberá incluir un sistema de reporteria integrado con al menos los siguientes reportes

predeterminados:

- Logins y eventos de administración
- Anchos de Banda y aplicaciones



- Reputación de clientes
  - Reportes por usuario
  - VPN
  - Redes inalámbricas
  - IPS
  - Amenazas
- Deberá incluir un completo sistema de reportes personalizables pudiendo realizar consultas complejas a la base de datos de registro de logs.
  - Subsistema de monitoreo especial para los túneles de VPN de tal forma que el área de operación puede monitorear desde una sola pantalla el estado de todos los túneles de VPN establecidos, administrados y operados desde la consola de administración.
  - Deberá soportar automatización y calendarización en la ejecución de reportes.
  - Deberá contar con un panel de monitoreo en tiempo real para las siguientes opciones:
    - Orígenes
    - Aplicaciones
    - Destinos
    - Sitios Web
    - Amenazas
    - Eventos de sistema
    - VPN (SSL / IPSEC)

### ***Licenciamiento y actualizaciones***

#### **\* Tamaño de licencia**

El licenciamiento de todas las funcionalidades que permita la administración de 110 dispositivos con posibilidad de crecimiento mediante la adición de licencias.



### \* Vigencia de licencia de actualización

La vigencia de las actualizaciones para los servicios de soporte y actualización de versiones debe proveerse por al menos 3 años.

### 6- Sistema de Reportería, Analisis y recolección de logs

Adquisición de un sistema de reporte, análisis y almacenamiento de bitácoras, que incluye capacidades de correlación y análisis de vulnerabilidades en la red para dispositivos de Administración Unificada de Amenazas (UTM por sus siglas en inglés, Unified Threat Management)

#### Funcionalidades:

- La solución propuesta deberá cumplir con las siguientes funcionalidades:
  - Sistema de Almacenamiento de Logs y Reportes.
  - Dispositivo tipo appliance de propósito específico, el cual también debe contar con la posibilidad de implementarse sobre ambientes virtuales.
- Sistema operativo propietario
- Interface de administración gráfica (GUI) vía Web (HTTPS)
- Interface de administración vía CLI (Línea de comando), vía ssh y consola serial
- Permite la definición de dominios administrativos independientes para dividir o segmentar el control de la información recibida y almacenada por dispositivo.



- Tiene la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativa.
- Permite la posibilidad de utilizar repositorio de datos externos (bases de datos)
- Permite integrar dispositivos para que reporten, y establezcan comunicaciones seguras con dichos dispositivos.
- Permite 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.
- Debe poder correr en plataformas de virtualización como VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM y Amazon Web Services (AWS)

#### **Generación de reportes:**

- Permite generar reportes personalizados, permite al administrador de la solución el 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)
- Genera reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.
- Genera reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por fuente y/o por destino.
- Genera reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.



- Permite de generar la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino
- Permite generar un reporte de las actividades administrativas (entradas de administradores, cambios de configuración) realizadas.
- Permite personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana.
- Permite especificar el período de tiempo específico para el cual el reporte va a ser obtenido, 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)
- Permite la calendarización de reportes.
- Permite generar reportes en formato PDF, HTML, XML y CSV.
- Tiene la opción de generar reportes en idioma inglés y en idioma español
- Permite enviar el reporte vía correo electrónico.

#### **Análisis forense y correlación:**

- Permite hacer búsquedas por username o dirección IP, para que toda la información almacenada de dicho username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.

#### **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



### ***Licenciamiento y actualizaciones***

#### **\* Tamaño de licencia**

El licenciamiento de todas las funcionalidades que permita recolectar hasta 6 GB de logs por día y debe permitir el crecimiento mediante la adición de licencias.

#### **\* Vigencia de licencia de actualización**

La vigencia de las actualizaciones para los servicios de soporte y actualización de versiones debe proveerse por al menos 3 años.

#### ***Especificaciones técnicas:***

- Almacenamiento: debe permitir almacenar hasta 3,2 TB de información.

#### ***7.- Servicios y Capacitación***

Se debe constar de servicios profesionales acordes a la implementación de la totalidad del equipamiento a proveer. Así mismo se debe realizar jornadas de capacitaciones, dentro de estas jornadas el contenido del curso debe ser orientado con opcional a certificación acerca del equipamiento propuesto como también del proyecto implementado, considerando también administración sobre plataforma de control de contenido y análisis. El curso debe cubrir aspectos de seguridad avanzados. Los temas incluirán características comúnmente en la infraestructura de redes, tales como enrutamiento avanzado, modo transparente, infraestructura redundante, avanzado IPsec VPN, IPS, SSO, la prevención de fuga de datos, diagnósticos y rendimiento de ajuste fino.



Los tópicos a tratar deben incluir también los fundamentos del uso un manager para la administración centralizada de la red de los dispositivos, donde se deben revisar estrategias de implementación que incluyen ADOMs únicas o múltiples, paquetes de políticas, los objetos compartidos, y aprovisionamiento de servidores de distribución local para los servidores de seguridad gestionados. Registrar los dispositivos conocidos y desconocidos mediante un analizador de red. Contenido sobre visualización en tiempo real con la información de registro histórico a partir de los dispositivos de la infraestructura, donde se realice una instrucción de como crear alertas para notificar a los administradores de eventos que se producen en los dispositivos registrados, definido privilegios administrativos. Contenido acerca de cómo realizar una evaluación de la vulnerabilidad de los host en la infraestructura, con un análisis del tráfico de red.

### **ETFWCASINOSM: Firewall Perimetral tipo UTM para casinos mediano**

**Unidades:** 2 (cluster de 2 equipos)

Adquisición de un sistema de seguridad informática perimetral que sea 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 en el presente documento.

Esta solución será utilizada para establecer una conexión vía VPN contra el sitio central y procesar el tráfico que se origine desde el casino hacia otros destinos.

#### ***Funcionalidades y Características del Sistema:***



### Características del dispositivo

- El dispositivo debe ser un equipo de propósito específico.
- Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". 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 de forma local ciertas consultas de acuerdo a la configuración del administrador.
- El equipo de seguridad 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.
- Debe contar con fuentes redundantes internas o externas para asegurar el funcionamiento ante posibles cortes de energía.
- La solución proporcionada debe contar con un formato rackeable de hasta 1 unidades de rack.

### Firewall



- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Por granularidad y seguridad, 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.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia 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),



- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
- El equipo 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.
- El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN
- La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.
- La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada
- La solución será capaz de integrar los servicios dentro de las 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
- La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo
- La solución 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
- El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.



- El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS
- La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o específica
- La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
- El dispositivo integrara 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 cuál de 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)
- Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento. En este modo, 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
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
- La solución podrá habilitar políticas de ruteo en IPv6
- La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6
- La solución 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 explícito
- Deberá ser capaz de integrar políticas con proxy explícito en IPv6
- La solución podrá restringir direcciones IPv6 en modo proxy explícito
- 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



- La solución 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 para trafico IPv6
- El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6
- La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface
- La solución deberá contar 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.
- Se debe soportar 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.
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.



- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSeC client-to-site.
- La VPN IPSeC deberá poder ser configurada en modo interface (interface-mode VPN)
- En modo interface, la VPN IPSeC deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de 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. En este modo, 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 algún 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, entendiéndose como 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 que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autenticación nuevamente.

### **Traffic Shapping / QoS**

- Capacidad de poder asignar parámetros de traffic shapping
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente
- Capacidad de poder definir ancho de banda garantizado
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo)



- 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 sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"
- Capacidad de 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.
- Debe ser posible 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. Esto significa que podrán 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.
- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
  - 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 “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo 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 appliance, 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 incluir 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" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)

### AntiSpam

- La capacidad antispam incluida deberá ser capaz de 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 incluida 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 listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
- 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
- En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de



etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

### Filtrado de URLs (URL Filtering)

- Facilidad para incorporar control de sitios a los cuales navegen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
- 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, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo 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 Filtraje 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 Youtube, bloqueando cualquier tipo de contenido no Educativo.
- 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 la página completa.
  2. Modo Proxy: La pagina 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.
- La funcionalidad de reputación busca que, al acceder a paginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una pagina de esta índole. De acuerdo a esto se

391



extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red.

- El sistema de filtrado de URLs debe incluir la 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 código en la configuración de filtrado de URLs del equipo para poder habilitar únicamente 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" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones 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 de 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. También podrá definirse el bloqueo 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:
  - 1. 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 utilizados. Dicha lista debe actualizarse de forma periódica por el fabricante.



- 2. 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.
- La funcionalidad 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 la detección de una posible fuga de información deben poder aplicarse el menos 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, la solución 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:
  1. Filtrado por tipo de archivo
  2. Filtrado por nombre de archivo
  3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.



4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.
5. 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**

- Lo solución debe soportar la capacidad de 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.
- Las 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 poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes 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

#### **Controlador Inalámbrico (Wireless Controller)**

- El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless
- En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación.
- Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection.
- El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs.
- Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.
- La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el tráfico wireless para detectar y reportar posibles intentos de intrusión.



- Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente.
- El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta.
- El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off.
- Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred.
- El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz grafica (GUI)
- El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota.
- El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión.
- El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricas dentro del mismo segmento de red.
- El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad,
- El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC



- El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletas, Laptops, PCs (tanto en Windows como en Linux)
- El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.

### **Filtrado de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea**

- Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).
- El dispositivo deberá 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.
- En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.
- La solución debe contar con un ALG (Application Layer Gateway) de SIP
- Debe poder hacerse 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 tráfico SSH en modo proxy explícito
- La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explícito 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**

- La solución 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 tráfico 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 la 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 tráfico 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
- Alta Disponibilidad en modo 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 y que forme 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. Este puerto debe estar 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 especificar 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 bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2
- Soporte de SNMP versión 3
- Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
- Soporte para 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 cuando ocurra 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 grafica.



- Contar con facilidades de administración a través de la interfaz grafica como listas de edición a través de click derecho.
- Contar con facilidades de administración a través de la interfaz grafica como 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.
- Contar con herramientas graficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

## Virtualización

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”
- La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus
- Se debe incluir la licencia para al menos 10 instancias virtuales dentro de la solución a proveer.
- 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.
- Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el tráfico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.

### **Análisis de Seguridad y Almacenamiento de Logs en la Nube**

- La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función.
- Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legítimo o ilegítimo, por medio de técnicas de Caja de Arena o Sandboxing.
- Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse.
- Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz.
- Permitir Monitoreo y alertas en tiempo real.
- Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis.
- Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.

### **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

### **3.- Licenciamiento y actualizaciones**

#### **\* Tamaño de licencia**

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.

#### **\* Vigencia de licencia de actualización**

La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos 3 años.

### **4.- Desempeño / Conectividad**

El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad



Numero de Interfaces Requeridas	4x 1GE SFP, 4x GE RJ45, 2x 1GE RJ45 para Management.
Throughput de Firewall (con paquetes de 1518/512/64 byte)	8 Gbps/8 Gbps/8 Gbps
Latencia de firewall (con paquetes de 64 byte)	3 $\mu$ s
Paquetes por Segundo procesados por el Firewall	12 Mpps
Throughput de VPN IPSec (con paquetes de 512 byte)	7 Gbps
Throughput de NGFW	1,5 Gbps
Throughput de IPS (HTTP/Enterprise Mix)	2,8 Gbps / 2 Gbps
Throughput de Inspección SSL	1.9 Gbps
Políticas de Firewall admitidas	10.000
Tuneles gateway to gateway	2.000
Tuneles client to gateway	10.000
Tuneles SSL	500
Throughput VPN SSL	350 Mbps
Sesiones Concurrentes	6 Millones
Nuevas sesiones / segundo	200.000
Storage (SSD)	120 GB



## **ETFWCASINOSC: Firewall Perimetral tipo UTM para casinos chico**

**Unidades:** 2 (cluster de 2 equipos)

Adquisición de un sistema de seguridad informática perimetral que sea 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 en el presente documento.

Esta solución será utilizada para establecer una conexión vía VPN contra el sitio central y procesar el tráfico que se origine desde la dependencia hacia otros destinos.

### ***Funcionalidades y Características del Sistema:***

#### **Características del dispositivo**

- El dispositivo debe ser un equipo de propósito específico.
- Basado en tecnología ASIC y que sea capaz de brindar una solución de "Complete Content Protection". 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).

406



- 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 de forma local ciertas consultas de acuerdo a la configuración del administrador.
- El equipo de seguridad 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.

## Firewall

- Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
- Por granularidad y seguridad, 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.



- Las reglas de firewall deberán poder tener limitantes y/o vigencia 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),
- La solución deberá tener la capacidad de balancear carga entre servidores. Esto es realizar una traslación de una única dirección a múltiples direcciones de forma tal que se distribuya el tráfico entre ellas.
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
- El equipo 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.
- El equipo deberá permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN
- La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.
- La solución de seguridad deberá permitir la creación de servicios de Firewall para implementar dentro de las políticas de seguridad y categorizarlos de manera personalizada



- La solución será capaz de integrar los servicios dentro de las 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
- La solución será capaz de habilitar o deshabilitar el paso de tráfico a través de procesadores de propósito específico, si el dispositivo cuenta con estos procesadores integrados dentro del mismo
- La solución 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
- El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.
- El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS
- La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o específica
- La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.
- El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados
- El dispositivo será capaz de ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico
- Tendrá la capacidad de hacer escaneo a profundidad de tráfico 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 cuál de 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)
- Soporte de ECMP con peso. En este modo el tráfico será distribuido entre múltiples rutas pero no en forma equitativa, sino en base a los pesos y preferencias definidas por el administrador.
- Soporte de ECMP basado en comportamiento. En este modo, 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
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
- La solución podrá habilitar políticas de ruteo en IPv6
- La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6
- La solución 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 explícito
- Deberá ser capaz de integrar políticas con proxy explícito en IPv6
- La solución podrá restringir direcciones IPv6 en modo proxy explícito
- 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
- La solución 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 contará 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 para tráfico IPv6
- El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6
- La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface
- La solución deberá contar 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 encontrará 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.
- Se debe soportar 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.
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSeC client-to-site.
- La VPN IPSeC deberá poder ser configurada en modo interface (interface-mode VPN)
- En modo interface, la VPN IPSeC deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de 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. En este modo, 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 algún 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, entendiéndose como 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 que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autenticación nuevamente.

## Traffic Shapping / QoS



- Capacidad de poder asignar parámetros de traffic shapping
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente
- Capacidad de poder definir ancho de banda garantizado
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo)
- 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 sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On"
- Capacidad de 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.
- Debe ser posible 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. Esto significa que podrán 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.



- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
  - 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 “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo 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 appliance, 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 incluir 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" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)

### **AntiSpam**

- La capacidad antispam incluida deberá ser capaz de 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 incluida 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 listas blancas y



listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).

- 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
- En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

#### **Filtrado de URLs (URL Filtering)**

- Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
- 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, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. Estos mensajes de remplazo 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 Filtraje 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 Youtube, bloqueando cualquier tipo de contenido no Educativo.
- 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 la página completa.
  2. Modo Proxy: La pagina 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.
- La funcionalidad de reputación busca que, al acceder a paginas de contenido no deseado (tales como Malware, pornografía, consumo de ancho de banda excesivo, etc) se asigne un puntaje a cada usuario o IP cada vez visita una pagina de esta índole. De acuerdo a esto se extrae los usuarios que infringen las políticas de filtrado con más frecuencia con el fin de detectar zombies dentro de la red.
- El sistema de filtrado de URLs debe incluir la 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" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a

419



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 de 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. También podrá definirse el bloqueo 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:
  - 1. 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.
  - 2. 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.
- La funcionalidad 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 la detección de una posible fuga de información deben poder aplicarse el menos 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, la solución 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:
  1. Filtrado por tipo de archivo
  2. Filtrado por nombre de archivo
  3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.
  4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.
  5. 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**

- La solución debe soportar la capacidad de 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 poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
- Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes 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

### **Controlador Inalámbrico (Wireless Controller)**

- El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless
- En modo de Controlador de Wireless tendrá la capacidad de configurar múltiples puntos de acceso (Access Points: APs) reales de forma tal de que se comporten como uno solo. Cómo mínimo deberá controlar los SSID, roaming entre APs, configuraciones de cifrado, configuraciones de autenticación.



- Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection.
- El controlador de Wireless tendrá la capacidad de configurar la asignación de direcciones IP mediante DHCP a las estaciones de trabajo conectadas a los APs.
- Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.
- La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el tráfico wireless para detectar y reportar posibles intentos de intrusión.
- Debe contar con un sistema de aprovisionamiento de usuarios invitados para red wifi, que permita la creación sencilla de accesos para invitados, por medio de un portal independiente.
- El equipo debe tener capacidad de que estos usuarios invitados con acceso inalámbrico, tengan la opción de colocar o no contraseña, con tiempo limitado y configurable para la expiración de la cuenta.
- El controlador inalámbrico debe estar en la capacidad de balancear la carga entre los puntos de acceso (Access Points) soportando por lo menos los siguientes métodos de balanceo: Access Point Hand-off, Frequency Hand-off.
- Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma red.
- El dispositivo deberá ser capaz de administrar los dispositivos wireless AP de la misma plataforma, tanto en consola CLI como a través de una interfaz gráfica (GUI)
- El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota.
- El dispositivo debe poder cifrar la información que se envía hacia los puntos de acceso de la misma plataforma, sobre los cuales se esté teniendo control y gestión.



- El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricas dentro del mismo segmento de red.
- El equipo debe tener la capacidad de reconocer y monitorear diferentes tipos de dispositivos de comunicación móvil como Smartphones Androide, Blackberry y Iphone; diferentes tipos de consolas de juego como Xbox, PS2, PS3, Wii, PSP; diferentes tipos de tabletas con SO Androide o tabletas Ipad,
- El equipo debe tener la capacidad de controlar el acceso a la red de los diferentes dispositivos antes mencionados a través de ACLs por MAC
- El equipo deberá permitir el crear diferentes niveles de acceso a la red en función del tipo de dispositivo que se conecte, siendo estos: Smartphones, Tabletats, Laptops, PCs (tanto en Windows como en Linux)
- El equipo debe permitir la separación de redes al menos entre usuarios internos e invitados, permitiendo la colocación de reglas en función de los dispositivos móviles conectados.

### **Filtrado de tráfico VoIP, *Peer-to-Peer* y Mensajería instantánea**

- Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).
- El dispositivo deberá 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.
- En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.
- La solución debe contar con un ALG (Application Layer Gateway) de SIP
- Debe poder hacerse 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 tráfico SSH en modo proxy explícito
- La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explícito 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**

- La solución 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 tráfico 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 la 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
- Alta Disponibilidad en modo 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 y que forme 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. Este puerto debe estar 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 especificar 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 bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2
- Soporte de SNMP versión 3
- Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
- Soporte para 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 cuando ocurra 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 grafica.
- Contar con facilidades de administración a través de la interfaz grafica como listas de edición a través de click derecho.
- Contar con facilidades de administración a través de la interfaz grafica como 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.
- Contar con herramientas graficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.

## Virtualización

- El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”
- La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus
- Se debe incluir la licencia para al menos 10 instancias virtuales dentro de la solución a proveer.
- 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.
- Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el tráfico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente.

### **Análisis de Seguridad y Almacenamiento de Logs en la Nube**

- La solución de seguridad debe contar con una solución en la nube que permita centralización de reportes, análisis de tráfico, administración de configuraciones, y almacenamiento de logs sin la necesidad de software o hardware adicional para esta función.
- Contar con funcionalidad de Análisis de archivos sospechosos en la nube en caso que no se cuente con suficiente información en la solución de seguridad para calificar el tráfico como legítimo o ilegítimo, por medio de técnicas de Caja de Arena o Sandboxing.
- Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse.
- Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz.
- Permitir Monitoreo y alertas en tiempo real.
- Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis.



- Debe permitir visualizar de manera sencilla que todos los equipos de seguridad perimetral gestionados cuenten con la misma versión de firmware o sistema operativo para garantizar la homogeneidad en la red.

### **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

### **3.- Licenciamiento y actualizaciones**

#### **\* Tamaño de licencia**

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.

#### **\* Vigencia de licencia de actualización**

La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS, Application Control y URL Filtering debe proveerse por al menos 3 años.

### **4.- Desempeño / Conectividad**

431



El equipo debe por lo menos ofrecer las siguientes características de desempeño y conectividad

Numero de Interfaces Requeridas	14x 1GE RJ45, 2x 1GE RJ45 para WAN
Throughput de Firewall (con paquetes de 1518/512/64 byte)	3,5 Gbps/3,5 Gbps/3,5 Gbps
Latencia de firewall (con paquetes de 64 byte)	4 $\mu$ s
Paquetes por Segundo procesados por el Firewall	5.3 Mpps
Throughput de VPN IPSec (con paquetes de 512 byte)	1 Gbps
Throughput de NGFW	22,5 Mbps
Throughput de IPS (HTTP/Enterprise Mix)	275 Mbps / 41 Mbps
Throughput de Inspección SSL	35 Mbps
Políticas de Firewall admitidas	5.000
Tuneles gateway to gateway	200
Tuneles client to gateway	1.000
Tuneles SSL	200
Throughput VPN SSL	35 Mbps
Sesiones Concurrentes	2 Millones



Nuevas sesiones / segundo	4.000
Storage (SSD)	32 GB

**ETSRVSTO : UPGRADE de infraestructura central de proceso y almacenamiento.**

### Cajón Blade Cisco USC

Nº Parte	Descripción	Duración Mantenimiento	Cant.
<b>UCS-SP-5108-AC</b>	UCS SP Select 5108 AC2 Chassis w/2208 IO, 4x SFP cable 3m	N/A	1
CAB-IR2073-C19-AR	IRSM 2073 to IEC-C19 14ft Argen	N/A	4
N20-FAN5	Fan module for UCS 5108	N/A	8
CON-SNT-5108AC	SMARTNET 8X5XNBD UCS SP Select 5108 AC2 Chassis w/2208 IO, 4	36	1
UCSB-PSU-2500ACDV	2500W Platinum AC Hot Plug Power Supply – DV	N/A	4
UCS-IOM-2208XP	UCS 2208XP I/O Module (8 External, 32 Internal 10Gb Ports)	N/A	2
UCSB-5108-PKG-HW	UCS 5108 Packaging for chassis with half width blades.	N/A	1
SFP-H10GB-	10GBASE-CU SFP+ Cable 3 Meter	N/A	4

433



Nº Parte	Descripción	Duración Mantenimiento	Cant.
CU3M			
N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis	N/A	1
N20-CBLKB1	Blade slot blanking panel for UCS 5108/single slot	N/A	8
N20-FW014	UCS 5108 Blade Chassis FW Package 3.1	N/A	1
N01-UAC1	Single phase AC power module for UCS 5108	N/A	1

### Servidor Blade Cisco UCS (hojas) 2 CPU 256 Gb RAM

Nº Parte	Descripción	Duración Mantenimiento	Cant.
<b>UCS-SP-B200M4-B-A2</b>	B200M4 Adv2 w/2xE52680v4,8x32GB,VIC1340	N/A	12
UCSB-LSTOR-BK	FlexStorage blanking panels w/o controller, w/o drive bays	N/A	24
UCS-CPU-E52680E	2.40 GHz E5-2680 v4/120W 14C/35MB Cache/DDR4 2400MHz	N/A	24
Nº Parte	Descripción	Duración Mantenimiento	Cant.



CON-SNT-B200BA2	SNTC 8X5XNBD, (Not sold standalone)B200M4 Adv2 w/2xE52680v4,	36	12
UCSB-MRAID12G	Cisco FlexStorage 12G SAS RAID controller with Drive bays	N/A	12
UCSB-MLOM-40G-03	Cisco UCS VIC 1340 modular LOM for blade servers	N/A	12
UCS-M4-V4-LBL	Cisco M4 - v4 CPU asset tab ID label (Auto-Expand)	N/A	12
UCSB-HS-EP-M4-F	CPU Heat Sink for UCS B200 M4/B420 M4 (Front)	N/A	12
UCSB-HS-EP-M4-R	CPU Heat Sink for UCS B200 M4/B420 M4 (Rear)	N/A	12
UCS-MR-1X322RV-A	32GB DDR4-2400-MHz RDIMM/PC4-19200/dual rank/x4/1.2v	N/A	96

#### Pack de discos para EMCVN4500 para 50 Tbytes de capacidad

Producto	Descripción	Cantidad
V4-2S15-600U	VNX2 600GB 15K SAS 25X2.5 DPE/DAE UPG	108
VNXB6GSDAE25F	VNXB 25X2.5 6G SAS EXP DAE-FIELD INST	4
V4-2S6FX-1600U	VNX 1600GB MLC SSD 25X2.5 DAE U/G	10
C13-PWR-4	2 C13 PWRCORDS W/ IRAM 2073 250V 10A	4
VNXBOEPERFTBU	VNXB OE PER TB PERFORMANCE UPGRADE	79

435



### Pack de discos para EMCDD2500 para 12 Tbytes de capacidad

Producto	Descripción	Cantidad
U-2500-AX	ADD 5X3TB SAS HDD, 15TB, DD2500, UPGRADE	1
U-REP-2500-CF	LICENSE, REPLICATOR, DD2500, UPGRADE=IA	1

### Software de Gestión de Virtualización VMWare

Item	Cantidad
VMware vSphere Essentials Plus Kit / Asistencia técnica, 24 horas al día, 7 días a la semana/ Soporte por 36 meses	8



## ANEXO IV

Venta estimada de máquinas año 2017													
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Central	\$ 179.878.660,00	\$ 176.381.660,00	\$ 144.274.602,00	\$ 89.395.680,00	\$ 81.477.886,00	\$ 84.572.451,00	\$ 109.685.226,00	\$ 101.491.557,00	\$ 120.894.715,50	\$ 120.894.715,50	\$ 120.894.715,50	\$ 120.894.715,50	\$ 1.450.736.586,00
Tandil	\$ 50.120.273,00	\$ 49.703.787,00	\$ 55.934.530,00	\$ 51.719.623,00	\$ 48.649.040,00	\$ 52.720.321,00	\$ 59.455.613,00	\$ 58.323.982,00	\$ 53.328.397,38	\$ 53.328.397,38	\$ 53.328.397,38	\$ 53.328.397,38	\$ 639.940.766,50
Monte Hermoso	\$ 10.835.220,00	\$ 9.841.820,00	\$ 5.316.321,00	\$ 4.008.311,00	\$ 2.595.516,00	\$ 3.197.503,00	\$ 3.821.372,00	\$ 3.666.320,00	\$ 5.410.547,88	\$ 5.410.547,88	\$ 5.410.547,88	\$ 5.410.547,88	\$ 64.926.574,50
Miramar	\$ 42.320.968,00	\$ 41.746.152,00	\$ 27.939.918,00	\$ 17.965.409,00	\$ 15.407.826,00	\$ 15.946.818,00	\$ 20.544.255,00	\$ 17.651.722,00	\$ 24.903.136,00	\$ 24.903.136,00	\$ 24.903.136,00	\$ 24.903.136,00	\$ 296.837.632,00
Tigre	\$ 278.597.790,00	\$ 264.467.825,00	\$ 292.435.243,00	\$ 293.766.075,00	\$ 271.062.200,00	\$ 301.417.766,00	\$ 359.861.216,00	\$ 322.188.762,00	\$ 297.976.359,63	\$ 297.976.359,63	\$ 297.976.359,63	\$ 297.976.359,63	\$ 3.575.716.315,50
Hermitage	\$ 62.540.067,00	\$ 67.727.836,00	\$ 56.059.299,00	\$ 45.603.591,00	\$ 38.180.407,00	\$ 41.863.462,00	\$ 51.665.052,00	\$ 48.045.065,00	\$ 51.460.597,63	\$ 51.460.597,63	\$ 51.460.597,63	\$ 51.460.597,63	\$ 617.527.171,50
Pinamar	\$ 2.438.754,00	\$ 2.011.019,00	\$ 715.213,00	\$ 416.183,00	\$ 123.392,00	\$ 142.612,00	\$ 208.976,00	\$ 158.377,00	\$ 776.940,75	\$ 776.940,75	\$ 776.940,75	\$ 776.940,75	\$ 9.323.289,00