MUNICIPALIDAD DE ESCAZÚ

PROVEEDURÍA

CONTRATACIÓN DIRECTA Nº 2016CD-000118-01

"CONTRATACIÓN DE EQUIPOS DE SEGURIDAD INFORMÁTICA PERIMETRAL"

Se recibirán ofertas hasta las 08:00 Horas Del día: Jueves 24 de noviembre de 2016.

En la oficina de Proveeduría: Ubicada en el edificio Anexo del Palacio Municipal

CAPÍTULO PRIMERO

Condiciones Específicas de la Contratación

1. GENERALIDADES

El Proceso Proveeduría de la Municipalidad de Escazú, invita a participar en la presente Contratación Directa de: **"*Contratación de Equipos de Seguridad Informática Perimetral*".** La oficina encargada del procedimiento y que proporcionará la información adicional necesaria respecto de las especificaciones y documentación relacionada con el presente concurso será el Proceso de Proveeduría Municipal. Cualquier aclaración o duda sobre las condiciones del cartel deben presentarse por escrito ante ese departamento, en forma personal o vía fax al número 2288 1365.

El Proceso Informática supervisará la correcta ejecución de los servicios para lo cual efectuará los controles de calidad respectivos. Asimismo, el Proceso de Informática es la dependencia encargada de recibir el bien.

El pliego de condiciones podrá obtenerse en forma digital en las Oficinas del Proceso Proveeduría de la Municipalidad de Escazú, para lo cual las personas interesadas deberán traer un dispositivo de almacenamiento USB libre de virus. Se advierte que, si el dispositivo USB se encuentra infectado, no se transferirá el archivo solicitado. El horario para gestionar la solicitud de información es de lunes a viernes de 7:30 a.m. a 4:00 p.m.

El presente concurso se rige de conformidad con los parámetros establecidos en este pliego de condiciones, en la Ley de Contratación Administrativa y su Reglamento.

2. ACLARACIONES Y MODIFICACIONES AL CARTEL

Toda solicitud de aclaración a las disposiciones del presente cartel, deberá efectuarse por escrito ante el Proceso Proveeduría de esta Municipalidad, dentro del primer tercio del plazo fijado para la recepción de ofertas.

La Administración se reserva el derecho de efectuar las modificaciones y / o aclaraciones a las condiciones o especificaciones del cartel, cuando se consideren necesarias, y se comunicaran a los potenciales oferentes oportunamente.

En caso de enviar la solicitud de aclaración o modificación por fax al número 2288-1365, debe remitirse el documento original en un plazo máximo de tres (3) días hábiles.

3. CONDICIONES GENERALES SEGUN LA LEY DE CONTRATACION ADMINISTRATIVA

3.1. Presentar facturación timbrada acorde al bien o servicio que presta.

3.2. La Administración no aceptará la presentación de ofertas en conjunto para la Contratación de Equipo de Seguridad Informática Perimetral.

3.3. Podrán presentarse ofertas de tipo consorcio para la Contratación de Equipo de Seguridad Informática Perimetral.

La Administración, según lo indicado en la Ley de Contratación Administrativa y el Reglamento a la Ley de Contratación Administrativa, aceptará Ofertas en Consorcio cumpliendo con las siguientes condiciones:

3.3.1. Se aceptarán la participación de dos (2) o más personas jurídicas en consorcio, siempre y cuando una sola de las personas físicas o jurídicas responda por ambas.

Los integrantes del consorcio responderán frente a la Administración de forma solidaria, como si fuesen una única contraparte.

3.3.2. Presentar copia certificada del acuerdo del consorcio en el que consten los términos que regularán las relaciones de las partes y de éstas con la Administración. El acuerdo consorcial cubrirá al menos los siguientes aspectos:

3.3.2.1. Se aceptarán la participación de dos (2) o más personas jurídicas en consorcio, siempre y cuando una sola de las personas físicas o jurídicas responda por ambas.

3.3.2.2. Los integrantes del consorcio responderán frente a la Administración de forma solidaria, como si fuesen una única contraparte.

3.3.2.2.1. Presentar copia certificada del acuerdo del consorcio en el que consten los términos que regularán las relaciones de las partes y de éstas con la Administración. El acuerdo consorcial cubrirá al menos los siguientes aspectos:

3.3.2.2.2. Calidades, incluido domicilio y medio para recibir notificaciones y capacidad de las partes.

3.3.2.2.3. Designación de los representantes, con poder suficiente para actuar durante la fase de estudio de ofertas, de formalización, de ejecución contractual y para trámites de pago.

3.3.2.2.4. Detalle de los aportes de cada uno de los miembros, sea en recursos económicos o bienes intangibles, como experiencia y de los compromisos y obligaciones que asumiría en fase de ejecución contractual.

3.3.2.2.5. El porcentaje de la participación de cada uno de ellos.

3.3.2.2.6. Plazo del acuerdo que deberá cubrir la totalidad del plazo contractual.

3.3.2.2.7. En dicho acuerdo debe dejarse constancia de que la responsabilidad de que cada una de los integrantes respecto de los trámites de consorcio y la ejecución del proyecto, es solidaria, así como en relación con las garantías que se ofrezcan en respaldo de tal ejecución.

3.3.2.2.8. Tal documento deberá ser otorgado por los representantes legales de cada una de los integrantes que presentan la oferta en consorcio y firmado por cada uno de ellos.

3.3.2.3. Igualmente, la Oferta, deberá estar firmada por cada uno de los representantes legales de los integrantes que la presentan de manera tal que sean legalmente obligatorios para todos los asociados.

3.3.2.4. Cada uno de los oferentes debe aportar las declaraciones y certificaciones solicitadas en el Capítulo Primero, punto N° 9 del pliego de condiciones.

3.3.2.5. En caso de que esta oferta en consorcio resulte adjudicada se rendirá una garantía de que respalde el cumplimiento de manera solidaria. Esta garantía de cumplimiento deberá cumplir con lo indicado en el Capítulo Primero, punto N° 11.1 del pliego de condiciones.

3.3.2.6. En caso de que esta oferta en consorcio resulte adjudicada, los involucrados deberán nombrar un único representante con facultades suficientes para asumir responsabilidades y recibir órdenes para y en nombre de todos los asociados de la oferta adjunta. Tal representante deberá ser representante legal de alguna de los integrantes que participan en la sociedad.

3.4. En caso de subcontratar, debe aportar lo dispuesto en el Artículo N° 69 del Reglamento a la Ley de Contratación Administrativa con su respectivo compromiso, para lo cual aportará un listado de las personas físicas o jurídicas subcontratadas. En ese detalle, se indicarán los nombres de todas las personas físicas o jurídicas con las cuales se va a subcontratar, incluyendo su porcentaje de participación en el costo total de la oferta y se aportará una certificación de los titulares del capital social y de los representantes legales de aquellas.

Además, la persona física o jurídica subcontratada debe aportar las declaraciones y certificaciones solicitadas en el Capítulo Primero, punto N° 9 del pliego de condiciones.

3.5. ***Presentación de las Ofertas***: Deberán presentarse en forma legible sin borrones ni tachaduras; en caso de error, la corrección correspondiente deberá efectuarse por medio de nota. La oferta deberá ser presentada antes de la hora de cierre de recepción en su sobre cerrado, con la siguiente leyenda:

MUNICIPALIDAD DE ESCAZU

CONRATACIÓN DIRECTA Nº 2016CD-000118-01

"CONTRATACIÓN DE EQUIPO DE SEGURIDAD INFORMÁTICA PERIMETRAL"

La no presentación de la oferta en sobre cerrado se entenderá bajo la exclusiva responsabilidad del proponente, no acarreará ningún vicio y tampoco relevará a los funcionarios de su deber de confidencialidad y custodia antes de la apertura.

3.6. La Administración no autoriza la presentación de ofertas por medios electrónicos de transmisión de datos como casilleros electrónicos, correos electrónicos u otros medios. En ningún caso se aceptará la presentación de ofertas por la vía telefónica.

3.7. Por el solo hecho de presentar oferta, se entenderá como una manifestación inequívoca de la voluntad del oferente de contratar con pleno sometimiento a las condiciones y especificaciones de este cartel, así como a las disposiciones legales y reglamentarias pertinentes.

3.8. Forman parte de la oferta, el original y los documentos que la acompañen. Una vez depositada la oferta en la Recepción de Proveeduría, no podrá ser retirada, entendiéndose que la misma pertenece a la Municipalidad.

3.9. Se permitirá la presentación de ofertas alternativas según lo estipulado en el Artículo Nº 70 del Reglamento a la Ley de Contratación Administrativa.

4. COPIAS

4.1. Cada oferta se compone de un original, y una copia debidamente firmadas en papel común, las cuales deben contener todos los documentos del original; en caso de discrepancias entre el original y la copia prevalece el original. No se aceptarán las ofertas con firmas escaneadas o digitalizadas.

4.2. La oferta debe ser firmada por la persona facultada legalmente, ya según lo indicado en el Artículo Nº 81 del Reglamento a la Ley de Contratación Administrativa la falta de la firma en una oferta no es un aspecto subsanable.

5. ESPECIES FISCALES

La persona física o jurídica adjudicada deberá pagar un 0.0025 del monto adjudicado en especies fiscales o su equivalente en un entero de gobierno, el cual debe entregarse para retirar el pago respectivo en el Proceso de Tesorería.

6. INDICAR EN LA OFERTA

6.1. Nombre de la Persona Jurídica proveedora.

La personería del firmante de ofertas de empresas extranjeras debe ser debidamente acreditada.

6.2. Dirección

6.3. Teléfono

6.4. Fax.

6.5. Vigencia de la oferta: La vigencia de la oferta es de treinta (30) días hábiles contados a partir de la fecha de apertura de esta contratación.

6.6. Precio: Los precios cotizados serán unitarios y definitivos y en moneda nacional o extranjera, sin sujeción a condición alguna no autorizada por este cartel. El monto deberá indicarse en números y letras coincidentes (en caso de divergencia entre esas dos formas de expresión, prevalecerá la consignada en letras), libre de todo tipo de impuestos.

Se deberá presentar el desglose de la estructura del precio junto con un presupuesto detallado y completo con todos los elementos que lo componen (entiéndase costos directos, indirectos, impuestos y utilidades)

6.7. Idioma: Las ofertas deberán ser presentadas en idioma español, no obstante, la literatura que la complemente podrá presentarse en otro idioma con la correspondiente traducción, donde se muestren las características y calidades del bien ofrecido.

El adjudicatario deberá realizar la traducción total al idioma español de toda la literatura que se aporte junto con la oferta.

6.8. Medio para recibir notificaciones: El oferente deberá indicar en la oferta medio para recibir notificaciones.

7. PLAZO PARA ADJUDICAR

El tiempo para adjudicar es de diez (10) días hábiles.

8. CERTIFICACIÓN Y DECLARACIONES JURADAS

El oferente deberá presentar en su propuesta:

8.1. Declaración jurada que se encuentra al día en el pago de los impuestos nacionales.

8.2. Declaración jurada que no está afectado por ninguna causal de prohibición (Artículo N° 22 y 22 Bis de la Ley de Contratación Administrativa)

8.3. Declaración jurada que no se encuentra inhabilitado para participar en procedimientos de Contratación Administrativa (Artículo N° 100 de la Ley de Contratación Administrativa)

8.4. Certificación que se encuentra al día en el pago de las obligaciones obrero patronales con la Caja Costarricense del Seguro Social, o bien, que tiene un arreglo de pago aprobado por ésta, vigente al momento de la apertura de las ofertas. En caso de no aportarse, la administración realizará impresión de la consulta en la página Web de ***SICERE*** el día de apertura.

En caso de que el oferente presente certificación de que no se encuentra inscrito como patrono ante la Caja Costarricense del Seguro Social, y del objeto licitado se derive tal obligación, la Administración le solicitará explicación, la que, en caso de resultar insatisfactoria de acuerdo a los lineamientos establecidos por la Caja Costarricense del Seguro Social, provocará la exclusión del concurso y la denuncia ante las autoridades correspondientes.

Así mismo, la Ley de Protección al Trabajador, en la modificación de la Ley Orgánica de la Caja Costarricense del Seguro Social, en el Artículo N° 74 establece *"..... los patronos y las personas que realicen total o parcialmente actividades independientes no asalariados deberán estar el día en el pago de las obligaciones con la Caja Costarricense del Seguro Social, conforme a la ley. Para realizar los siguientes trámites administrativos, será requisito estar al día en el pago de las obligaciones de conformidad con el Artículo N° 3 de esta Ley (...) Participar en cualquier proceso de contratación pública regulado por la Ley de Contratación Administrativa o por la Ley de Concesión de Obra Pública. En todo contrato administrativo deberá incluirse una cláusula que establezca como incumplimiento contractual, el no pago de las obligaciones con la seguridad social..."*

Por lo tanto, toda persona física o jurídica que es oferente – incluye a los representantes de casas extranjeras – en los concursos para la venta de bienes y servicios deberá declarar bajo fe de juramento su condición de trabajador independiente debidamente afiliado a la Caja Costarricense del Seguro Social y presentar el último recibo de pago.

8.5. Certificación que se encuentra al día en el pago con las obligaciones con el ***FODESAF***, o bien, que tiene un arreglo de pago aprobado por la Dirección General de Desarrollo Social y Asignaciones Familiares, vigente al momento de la apertura de las ofertas. En caso de no aportarse, la administración realizará impresión de la consulta en la página Web del ***Ministerio de Trabajo y Seguridad Social*** el día de apertura.

8.6. Aportar constancia original, emitida por el Instituto Nacional de Seguros, en el cual se valide la existencia de la Póliza del Seguro de Riesgos del Trabajo vigente y al día ante el Proceso Proveeduría acorde con los trabajos a realizar en concordancia con la actividad económica que ampare los trabajos a realizar. ***El recibo póliza no sustituye la constancia indicada anteriormente***.

9. LEGITIMACIÓN DEL ADJUDICATARIO

La persona jurídica que resulte ***adjudicada*** deberá aportar la siguiente documentación:

9.1. *Personas Jurídicas*

Deberá presentar copia de la cédula jurídica y certificado notarial original con no más de dos meses de emitida en la que indique:

9.1.1. Quién (es) ostentan la representación judicial y extrajudicial de la compañía, indicando sus calidades y si pueden actuar en forma conjunta o separada.

9.1.2. La naturaleza y propiedad de las acciones.

9.1.3. Las citas de inscripción en el Registro Público, de la sociedad, del personero acreditado y el domicilio social.

9.1.4. En caso de que las acciones pertenezcan a una o varias personas jurídicas, deberá indicarse el nombre de los accionistas de estas.

9.2. *Extranjeros*

9.2.1. El oferente extranjero se entiende sometido a las leyes y a los tribunales de la República, en todo lo concerniente a los trámites y ejecución del contrato, debiendo manifestarlo en forma expresa en su propuesta.

9.2.2. Queda entendido que el adjudicado extranjero deberá considerar la normativa legal que le afecte.

9.2.3. Los documentos solicitados, en caso de otorgarse por autoridades extranjeras, deberán presentarse legalizados de acuerdo con la Ley de Seguridad Consular de Costa Rica o autenticadas por un notario público costarricense actuando en el extranjero (en caso de ser necesario)

9.2.4. Aportar ***Documento de Identificación de Migración y Extranjería (DIMEX)***. Documento emitido por la Dirección General de Migración y Extranjería para personas físicas extranjeras residentes y aquellas acreditadas con una categoría especial.

10. GARANTIAS

10.1.CUMPLIMIENTO

El o los adjudicatarios deben presentar una garantía de cumplimiento del 8% (ocho por ciento) sobre el monto total adjudicado, con una vigencia de sesenta días (60) días hábiles después de recibidos los servicios por el Proceso Informática.

Por lo anterior, se le recuerda a la persona jurídica adjudicada que la jefatura del Proceso Informática, o quien se encuentre en su lugar, será el responsable durante la ejecución del contrato así como de su administración, y también de que la garantía de cumplimiento se mantenga vigente durante el tiempo de ejecución del servicio más sesenta (60) días hábiles (mencionados en el párrafo anterior), tomando en consideración si existen suspensiones, prórrogas o atrasos, dado que los mismos son aspectos determinantes, pues extienden la fecha de la entrega definitiva y por ende se hace necesario que dicha jefatura solicite cuando corresponda la ampliación de la vigencia de dicha garantía.

La persona jurídica adjudicada deberá presentar esa garantía en un plazo máximo de cinco (5) días hábiles, contados a partir de la firmeza del acto de adjudicación en el Sub Proceso de Tesorería Municipal y aportar copia a la Proveeduría de la Municipalidad de Escazú.

10.2.FORMA DE RENDIR LAS GARANTIAS

10.2.1. La garantía deberá entregarse ante el Sub Proceso de Tesorería de la Municipalidad de Escazú, ubicadas en el edificio anexo del Palacio Municipal (Antiguo Centro de Salud), en su horario ordinario de 7:30 a.m. a 4:00 p.m. de lunes a viernes.

10.2.2. La garantía se rendirá de conformidad con lo estipulado por el Artículo N° 42 y el Artículo Nº 46 bis del Reglamento a la Ley de Contratación Administrativa. Además de la garantía se debe presentar en el Sub Proceso Tesorería, copia del oficio mediante el cual se les solicitó la presentación de la garantía.

10.2.3. Cuando la garantía que se va a aportar es dinero en efectivo y se trata de colones costarricenses, éste deberá depositarse en la cajas recaudadoras de la Municipalidad de Escazú (incluir copia del recibo dentro de la oferta para el caso de garantías de participación) o mediante transferencia bancaria o depósito en la cuenta número ***100-01-035-000676-6*** del Banco Nacional de Costa Rica, con indicación clara y precisa del día y hora en que se realiza, quien es el garantizado, su plazo de vigencia, número y nombre del concurso al que se refiere (de igual forma incluir copia del comprobante de ingreso dentro de la oferta para el caso de garantías de participación).

10.2.4. Cuando se trate de dólares de los Estados Unidos de Norteamérica, deberá depositarse en la cuenta ***100-02-171-000466-2*** del Banco Nacional de Costa Rica, con indicación clara y precisa del día y hora en que se realiza, quien es el garantizado, su plazo de vigencia, número y nombre del concurso al que se refiere (de igual forma incluir copia del comprobante de ingreso dentro de la oferta para el caso de garantías de participación).

10.2.5. Para el caso de las cartas de garantía y de títulos valores transmisibles por endoso, éstos junto con los cupones, debidamente endosados a favor de la Municipalidad de Escazú, deberán depositarse antes de la fecha y hora límite señalados como plazo de vencimiento para la recepción de las ofertas, en el Sub Proceso Tesorería de la Municipalidad de Escazú.

10.2.6. El oferente deberá presentar junto con el original dos (2) copias, para que el Sub Proceso Tesorería coloque el sello de recibido del documento que depositó como garantía el cual quedará en custodia en el Sub Proceso Tesorería, así como el original de la estimación del operador de bolsa cuando corresponda.

10.2.7. Cuando se trate de títulos valores, el monto de la garantía a considerar para verificar si la cuantía satisface el monto requerido, será el de la respectiva estimación del operador de bolsa aportada.

10.2.8. Tanto la garantía de participación como de cumplimiento, podrán rendirse mediante depósito de bono de garantía de instituciones aseguradoras reconocidas en el país, o de uno de los Bancos del Sistema Bancario Nacional o el Banco Popular de Desarrollo Comunal; certificados de depósito a plazo, bonos del Estado o de sus instituciones, cheques certificados o de gerencia de un banco del Sistema Bancario Nacional.

10.2.9. La información mínima que deben contener y que debe ser corroborada por el oferente y / o adjudicatario, es la siguiente:

10.2.9.1. Cartas de garantía:

10.2.9.1.1. - Banco emisor.

10.2.9.1.2. - Tipo de garantía

10.2.9.1.3. - Número de Documento (Carta de Garantía).

10.2.9.1.4. - Monto de la Garantía en números y letras.

10.2.9.1.5. - Nombre del Oferente (a quien está garantizando).

10.2.9.1.6. - Número de identificación del oferente (a quien está garantizando)

10.2.9.1.7. - A favor de la Municipalidad de Escazú.

10.2.9.1.8. - Número de licitación o contratación.

10.2.9.1.9. - Título de la licitación o contratación.

10.2.9.1.10. - Plazo de vigencia de la garantía.

10.2.9.2. ***Títulos Valores***: A diferencia de los otros documentos los títulos valores no contienen toda la información que se requiere, por lo que quien los entregue en la Oficina de Valores, deberá conocerla e indicar los datos que corresponda, como son:

10.2.9.2.1. Tipo de garantía

10.2.9.2.2. Nombre del Oferente (a quien está garantizando).

10.2.9.2.3. Número de identificación del oferente (a quien está garantizando)

10.2.9.2.4. A favor de la Municipalidad o endosado a su favor.

10.2.9.2.5. Número de licitación o contratación.

10.2.9.2.6. Título de la licitación o contratación.

10.2.9.2.7. Se entenderá que el plazo de vigencia se mantiene hasta que sea procedente su devolución.

10.2.9.3. ***Los bonos y certificados*** se recibirán por su valor de mercado y deberán acompañarse de la estimación efectuada por un operador de alguna de las bolsas legalmente reconocidas. Se exceptúan de presentar estimación, los certificados de depósito a plazo emitidos por bancos estatales, cuyo vencimiento ocurra dentro del mes siguiente a la fecha en que se presenta. No se reconocerán intereses por las garantías mantenidas en depósito por la Administración; sin embargo, los que devenguen los títulos hasta el momento en que se ejecuten, pertenecen al dueño.

10.2.9.4. ***Cheques Certificados o de Gerencia***: Al igual que los títulos, los cheques no contienen toda la información que se requiere, por lo que quien los entregue en la Tesorería, deberá conocerla e indicar los datos que corresponda, como son:

10.2.9.4.1. Tipo de garantía.

10.2.9.4.2. Nombre del Oferente (a quien está garantizando).

10.2.9.4.3. Número de identificación del oferente (a quien está garantizando)

10.2.9.4.4. A favor de la Municipalidad o endosado a su favor.

10.2.9.4.5. Número de licitación o contratación.

10.2.9.4.6. Título de la licitación o contratación.

10.2.9.4.7. Plazo de vigencia de la garantía.

10.3.PRÓRROGAS, ADENDAS Y ENMIENDAS

10.3.1. Cuando por alguna razón sea necesario realizar prórrogas, adendas y / o enmiendas a las garantías existentes, los documentos que se aporten como garantía deben cumplir lo indicado en los puntos anteriores para el documento que van a presentar y adicionalmente debe indicarse:

10.3.1.1. El número de garantía que se prorroga, adenda o corrige.

10.3.1.2. Tipo de garantía.

10.3.1.3. Nombre del Oferente (a quien está garantizando).

10.3.1.4. Número de identificación del oferente (a quien está garantizando)

10.3.1.5. Número de licitación o contratación.

10.3.1.6. Título de la licitación o contratación.

10.3.2. Se aclara lo siguiente:

10.3.2.1. El Sub Proceso Tesorería no recibirá dentro de las garantías documentos como: Cinta de pago, comprobantes de Depósito a Cuentas Corrientes o de Ahorros, otros.

10.3.2.2. Se reitera que el caso de Cheques Certificados o de Gerencia y Títulos Valores, que no contienen en sí mismos la información que se requiere, por lo que deberá presentar al Sub Proceso Tesorería, copia del oficio mediante el cual se les solicitó la presentación de la garantía.

10.3.2.3. Si el interesado extravía las fotocopias que le entregó al Sub Proceso Tesorería o al Proceso Proveeduría en el proceso de recepción de la garantía, el funcionario del Sub Proceso Tesorería o del Proceso Proveeduría, le podrá suministrar una nueva copia, pero el cliente deberá cubrir el costo de las fotocopias.

10.3.2.4. Salvo manifestación expresa en contrario del depositante, tratándose de títulos valores y dinero en efectivo, se entiende que al ser depositados mantienen su vigencia hasta que sea procedente su devolución.

10.3.2.5. La garantía de cumplimiento, puede rendirse en cualquier moneda extranjera o bien en su equivalente en moneda nacional, al tipo de cambio de referencia para la venta, calculado por el Banco Central de Costa Rica, vigente al día anterior a la presentación de la oferta o la suscripción del contrato, según corresponda. En este último caso el contratista está obligado a mantener actualizado el monto de la garantía, por las variaciones de tipo de cambio que le puedan afectar.

10.4.DEVOLUCION DE GARANTIAS

10.4.1. La garantía de participación será devuelta a petición del interesado. La solicitud para devolución de la garantía deberá presentarse ante el Proceso Proveeduría quien coordinará con el Sub Proceso Tesorería, si la garantía fue aportada en dinero en efecto, el Proceso Proveeduría solicitará por escrito al Sub Proceso Contabilidad la confección del cheque, previa solicitud del dueño de dicha garantía con la presentación del comprobante original emitido por las cajas recaudadoras municipales o bancarias, todo con copia la expediente de contratación.

10.4.2. La garantía de cumplimiento será devuelta a petición del interesado ante el área técnica respectiva como administrador del contrato, quien hará la solicitud de devolución por escrito al Sub Proceso Tesorería o al Sub Proceso Contabilidad según corresponda.

10.4.3. Para cualquiera de los casos, devolución de garantía de participación o de cumplimiento, el interesado deberá presentar ante el Proceso Proveeduría o el área técnica según corresponda, lo siguiente:

10.4.3.1. Cuando se trata de personas físicas:

10.4.3.1.1. Carta donde solicita de manera formal de devolución de la garantía debidamente suscrita con número de cédula de identidad. Si la garantía va a ser retirada por una persona autorizada, la solicitud debe presentarse autenticada por un notario, caso contrario no se tramitará la solicitud.

10.4.3.1.2. Cuando se trate de dineros depositados en efectivo deberá adjuntar el recibo original y el dinero se devolverá mediante cheque o se depositará mediante transferencia en la cuenta bancaria que indique el proveedor, por lo que debe aportar copia de la constancia de cuenta cliente del Banco donde tiene la cuenta en la cual desea que se le realice la transferencia.

10.4.3.1.3. Esta cuenta debe estar a nombre del proveedor y debe ser en el mismo tipo de moneda, en la que presentó la garantía de participación o de cumplimiento.

10.4.3.1.4. En la solicitud debe indicar el nombre y calidades de la persona autorizada para retirar la garantía (en caso de que autorice al alguien para su retiro).

10.4.3.1.5. - Fotocopia de la cédula de identidad del proveedor y fotocopia de la cédula de la persona autorizada para el retiro.

10.4.3.1.6. Original del depósito realizado en las cajas recaudadores municipales o bancarias, en el cual conste el sello de recibido, si la garantía fue en dinero en efectivo.

10.4.3.1.7. - Si la garantía va a ser retirada por una persona autorizada, la solicitud debe presentarse autenticada por un notario, caso contrario no se tramitará la solicitud.

10.4.3.2. Cuando se trata de personas jurídicas:

10.4.3.2.1. Carta donde solicita de manera formal de devolución de la garantía, firmada por el Representante Legal de la empresa y número de cédula. Si la garantía va a ser retirada por una persona autorizada, la solicitud debe presentarse autenticada por un notario, caso contrario no se tramitará la solicitud.

10.4.3.2.2. Cuando se trate de dineros depositados en efectivo, el dinero se devolverá mediante cheque o se depositará mediante transferencia en la cuenta bancaria que indique el proveedor, por lo que debe aportar copia de la constancia de cuenta cliente del Banco donde tiene la cuenta en la cual desea que se le realice la transferencia. Esta cuenta debe estar a nombre del proveedor y debe ser en el mismo tipo de moneda en la que presentó la garantía.

10.4.3.2.3. En la solicitud debe indicar el nombre y calidades de la persona autorizada para retirar la garantía (en caso de que autorice al alguien para su retiro).

10.4.3.2.4. Fotocopia de la cédula de identidad de la persona autorizada para el retiro, (en caso de que no esté aportada en el Registro de Proveedores).

10.4.3.2.5. Fotocopia de la personería jurídica de la empresa

10.4.3.2.6. Original del depósito realizado en las cajas recaudadores municipales o bancarias, en el cual conste el sello de recibido, si la garantía fue en dinero en efectivo.

10.4.3.2.7. Indicar medio idóneo para dar aviso de la aprobación de la solicitud, correo electrónico, fax, etc.

10.4.3.2.8. Si la garantía va a ser retirada por una persona autorizada, la solicitud debe presentarse autenticada por un notario, caso contrario no se tramitará la solicitud.

10.4.3.2.9. Cuando la garantía a retirar sea un documento por endoso, el proveedor deberá presentarse ante el Sub Proceso Tesorería para su retiro hecha previamente la solicitud de devolución.

11. ELEGIBILIDAD

La elegibilidad de las ofertas queda condicionada a que la misma se ajuste a las condiciones establecidas en el presente cartel, así como lo estipulado en el Reglamento a la Ley de Contratación Administrativa y la Ley de Contratación Administrativa.

12. CLAUSULA DE DESEMPATE

En caso de presentarse empate en la calificación se utilizarán los siguientes criterios para desempate:

12.1. Se otorgará una puntuación adicional a las PYME que han demostrado su condición a la Administración, según lo dispuesto en el Reglamento a la Ley de Contratación Administrativa, la Ley Nº 8262 y sus reglamentos. La puntuación a asignar, será la siguiente:

12.1.1. PYME de industria, cinco (5) puntos

12.1.2. PYME de servicio, cinco (5) puntos

12.1.3. PYME de comercio, dos (2) puntos

12.2. En caso de que el empate persista se definirá aplicando el siguiente criterio:

12.2.1. La oferta de menor precio total cotizado.

12.3. De continuar el empate se procederá a realizar una rifa en presencia de las partes en el Proceso Proveeduría de la Municipalidad de Escazú.

13. CONDICIONES GENERALES PARA LOS CONTRATOS

13.1. La persona jurídica adjudicada deberá suscribir un contrato administrativo, cuya fecha de inicio se comunicará por escrito una vez obtenida su aprobación interna por parte del Proceso de Asuntos Jurídicos de esta Municipalidad.

13.2. Al contrato que se firme le será aplicable lo dispuesto en la Ley de Contratación Administrativa y demás instrumentos jurídicos sobre la materia, por tal motivo se tienen por incorporados.

13.3. La firma del contrato se realizará en el Proceso Proveeduría de la Municipalidad por parte del contratista. Será suscrito por quien ostente la respectiva representación legal en el plazo señalado por la Administración para este efecto.

13.4. Si existieren modificaciones respecto al representante legal, deberá ser presentada mediante certificación de un notario público, dicha modificación donde se señale la nueva persona que ostenta la representación legal de la empresa, o que tiene pleno poder para ello. Para efectos de la firma se exigirá la cédula de identidad vigente o documento de identificación vigente (cédula de residencia, pasaporte, otro)

13.5. El contrato empezará a regir después de que sea aprobado por el Proceso Asuntos Jurídicos de la Municipalidad de Escazú, para lo cual se contará con la orden de inicio del Proceso Informática.

14. CESIÓN DEL CONTRATO

14.1. Los derechos y obligaciones derivados de un contrato en ejecución o listo para iniciarse, podrán ser cedidos a un tercero, siempre que no se trate de una obligación personalísima.

14.2. En todo caso la cesión debe ser autorizada por la Administración mediante acto debidamente razonado, en el que al menos analizará:

14.2.1. Causa de la cesión.

14.2.2. El cumplimiento por parte del cesionario de las principales condiciones legales, técnicas y financieras solicitadas en el cartel.

14.2.3. Que el cesionario no esté afectado por alguna causal de prohibición.

14.2.4. Ventajas de la cesión de frente a resolver el contrato.

14.2.5. Eventuales incumplimientos del cedente hasta el momento y medidas administrativas adoptadas.

14.3. Si la cesión excede el cincuenta (50) por ciento del objeto contractual, independientemente del avance en su ejecución, deberá ser autorizada por la Contraloría General de la República de la República, quien resolverá dentro del décimo día hábil una vez presentada la solicitud. La petición de la Administración deberá contener como mínimo la solicitud formulada por el cedente; aceptación del cesionario y cualquier documentación que resulte pertinente en relación con sus condiciones, cartel y resolución motivada de la Administración.

14.4. El cesionario queda subrogado en todos los derechos y obligaciones que corresponderían al cedente y este quedará libre de todas las obligaciones con la Administración. En el supuesto de que la cesión genere modificaciones contractuales éstas seguirán los procedimientos comunes establecidos al efecto.

15. CESIÓN DE FACTURAS

15.1. Los derechos de cobro frente a la Administración, podrán cederse en cualquier momento, sin que sea necesario el consentimiento de ésta, ni de la Contraloría General de la República. Sin embargo, deberá informarse a la entidad una vez que la cesión sea convenida, sin detrimento de los montos que por concepto de multas y cláusulas penales se deban resarcir con dicho pago, los cuales se deducirán automáticamente del monto. Antes de esa comunicación cualquier pago hecho a nombre del contratista surtirá efecto liberatorio.

La Administración, no podrá negarse a pagar al cesionario, pero si podrá oponer la excepción de falta de cumplimiento o cumplimiento defectuoso de lo pactado.

La cesión de pago aceptada por la Administración, no exonera al contratista de sus obligaciones y tampoco convierte al cesionario en parte contractual. El cesionario del crédito asume por completo el riesgo por el no pago de la obligación por parte de la Administración, originado en las excepciones antes dichas.

Carecen de efecto legal las leyendas incluidas en las facturas comerciales que supongan aceptación del objeto contractual o renuncia a reclamos posteriores derivados de la simple recepción del documento de cobro.

15.2. Para gestionar el trámite de pago de facturas de esta Municipalidad las personas físicas o jurídicas, que vía contratos de cesión adquieran los derechos de crédito de aquellos terceros cuyo deudor sea la Municipalidad de Escazú, con tres (3) días hábiles de antelación a la presentación de la factura original ante el Proceso Cultura, se deberá cumplir con los siguientes requisitos:

15.2.1. Se deberá presentar la solicitud formal dirigida a la Jefatura del Proceso de Recursos Financieros, presentado copia de la personería jurídica vigente, indicación de los terceros autorizados para realizar los trámites de cesión de facturas y firmas autenticadas de los autorizados.

15.2.2. Aporte el testimonio de escritura del contrato de cesión de factura mediante el cual se trasladan los derechos de crédito a un tercero o el contrato entre partes con fecha cierta, según las formalidades del Código Civil, en original.

15.2.3. Los testimonios de escritura pública, además de los requisitos del Código Civil, deben contener los datos personales del cedente y cesionario, el número de factura cedida, fecha de la factura, monto bruto y liquido de la factura, número del procedimiento de contratación administrativa, orden de compra y descripción del objeto de la cesión. La estimación del contrato deber ser igual a la sumatoria de los montos brutos de las facturas cedidas e indicación exacta del número de cuenta bancaria y número de cuenta cliente en la cual la Municipalidad debe hacer efectivo el pago del crédito.

La forma de pago se ajustará a lo indicado en el punto Nº 16 del Capítulo Segundo del pliego de condiciones.

15.2.4. En los contratos privados, además de la información indicada en el punto anterior, se debe adjuntar fotocopia certificada de la personería jurídica vigente, fotocopia certificadas de las cédulas de identidad en caso de personas físicas, fotocopia de las cédulas de identidad de los representantes legales y certificación de la cuenta cliente emitida por la respectiva institución financiera.

Las firmas deberán venir debidamente autenticadas por un notario público en papel de seguridad y adjuntan la fecha cierta del respectivo contrato de cesión, acatando lo dispuesto por el Consejo Superior Notarial mediante la normativa que se indica a continuación:

15.2.4.1. Lineamientos para el Ejercicio del Servicio Notarial, publicado en el Diario Oficial La Gaceta Nº 97, Alcance Nº 93, del veintidós de mayo de dos mil trece.

15.2.4.2. Modificación, Reforma y Adición a los Lineamientos para el Ejercicio del Servicio Notarial, Acuerdo Nº 2014 – 003 – 007, publicado en el Diario Oficial La Gaceta Nº 51 el trece de marzo de dos mil catorce.

15.2.4.3. Reforma al Artículo Nº 32 de los Lineamientos para el Ejercicio del Servicio Notarial, Acuerdo Nº 2014 – 016 – 008, publicado en el Diario Oficial La Gaceta Nº 192 del siete de octubre de dos mil catorce.

16. OBSERVACIONES FINALES

16.1. Las condiciones específicas del objeto contractual son responsabilidad directa del área solicitante y técnica, no del Proceso Proveeduría. Todo a la luz del Principio de Eficiencia y Eficacia que rige la materia de Contratación Administrativa.

16.2. El Proceso Proveeduría realizará la revisión de forma general, la evaluación realizada por las áreas solicitante y técnica. De forma de que, si se detectan inconsistencias en el análisis, será retomado.

16.3. Todo oferente debe cumplir con todos los aspectos estipulados en el cartel.

16.4. El oferente debe participar en todos los renglones, se adjudicará al mejor calificado en forma global.

16.5. La Administración se reserva el derecho de adjudicar parcial o totalmente, mejor precio global según su conveniencia por lo cual el oferente debe indicar precios unitarios y totales según lo ofrecido.

16.6. En caso fortuito la administración recurrirá a las razones de lógica y al Principio de Buena Fe entre las partes.

Atentamente,

Cira Castro Myrie
Proveeduría

CAPÍTULO SEGUNDO

Objeto Contractual, Requisito y Especificaciones Técnicas

1. OBJETIVO GENERAL

A través del Plan Anual Operativo para este período 2016, se incluyó el presupuesto correspondiente y la justificación para llevar a cabo la presente contratación.

2. SUMINISTROS REQUERIDOS

2.1. *Renglón Nº 1: Contratación de Equipo de Seguridad Informática Perimetral para Palacio Municipal*

Se requiere gestionar la adquisición de una persona jurídica que brinde el suministro de un sistema de seguridad informática perimetral, del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), con las siguientes características ***mínimas***:

2.1.1.*Funcionalidades y Características del Sistema a nivel general:*

2.1.1.1. El dispositivo debe ser un equipo de propósito específico.

2.1.1.2. 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.

2.1.1.3. Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).

2.1.1.4. Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).

2.1.1.5. El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red.

2.1.1.6. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.

2.1.1.7. El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.

2.1.1.8. 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.

2.1.2.*Funcionalidades y Características del Sistema a Firewall*

2.1.2.1. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.

2.1.2.2. 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.

2.1.2.3. Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.

2.1.2.4. 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

2.1.2.5. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.

2.1.2.6. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo.

2.1.2.7. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)

2.1.2.8. Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.

2.1.2.9. Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)

2.1.2.10. Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.

2.1.2.11. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.

2.1.2.12. 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),

2.1.2.13. 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.

2.1.2.14. En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID

2.1.2.15. 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.

2.1.2.16. 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.

2.1.2.17. 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

2.1.2.18. La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.

2.1.2.19. 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

2.1.2.20. La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente

2.1.2.21. El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas

2.1.2.22. 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

2.1.2.23. 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

2.1.2.24. El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.

2.1.2.25. El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS

2.1.2.26. La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica

2.1.2.27. La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.

2.1.2.28. El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados

2.1.2.29. El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico

2.1.2.30. Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis

2.1.2.31. La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH

2.1.3.*Funcionalidades y Características del Sistema en Conectividad y Sistema de ruteo*

2.1.3.1. Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.

2.1.3.2. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.

2.1.3.3. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.

2.1.3.4. Soporte a políticas de ruteo (policy routing).

2.1.3.5. 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

2.1.3.6. Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS

2.1.3.7. Soporte a ruteo dinámico RIPng, OSPFv3

2.1.3.8. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.

2.1.3.9. Soporte de ECMP (Equal Cost Multi-Path)

2.1.3.10. 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.

2.1.3.11. 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.

2.1.3.12. Soporte a ruteo de multicast

2.1.3.13. La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

2.1.3.14. La solución podrá habilitar políticas de ruteo en IPv6

2.1.3.15. La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6

2.1.3.16. 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

2.1.3.17. 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

2.1.3.18. El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6

2.1.3.19. El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explicito

2.1.3.20. Deberá ser capaz de integrar políticas con proxy explícito en IPv6

2.1.3.21. La solución podrá restringir direcciones IPv6 en modo proxy explicito

2.1.3.22. Deberá hacer NAT de la red en IPv6

2.1.3.23. La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT

2.1.3.24. Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo

2.1.3.25. 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

2.1.3.26. La solución contara con una base de administración de información interna generada por sesiones sobre IPv6

2.1.3.27. Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6

2.1.3.28. El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6

2.1.3.29. La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface

2.1.3.30. La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad

2.1.3.31. El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrará el archivo de configuración

2.1.3.32. El dispositivo podrá hacer la función como servidor DHCP IPv6

2.1.3.33. La solución será capaz de configurar la autenticación por usuario por interface en IPv6

2.1.4.*Funcionalidades y Características del Sistema en VPN IPSec / L2TP / PPTP*

2.1.4.1. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)

2.1.4.2. Soporte para IKEv2 y IKE Configuration Method

2.1.4.3. Debe soportar la configuración de túneles PPTP

2.1.4.4. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.

2.1.4.5. Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits

2.1.4.6. Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.

2.1.4.7. Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.

2.1.4.8. Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.

2.1.4.9. La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)

2.1.4.10. 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.

2.1.4.11. Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

2.1.5.*Funcionalidades y Características del Sistema en VPN SSL*

2.1.5.1. Capacidad de realizar SSL VPNs.

2.1.5.2. Soporte a certificados PKI X.509 para construcción de VPNs SSL.

2.1.5.3. 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.

2.1.5.4. Soporte de renovación de contraseñas para LDAP y RADIUS.

2.1.5.5. Soporte a asignación de aplicaciones permitidas por grupo de usuarios

2.1.5.6. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.

2.1.5.7. 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.

2.1.5.8. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)

2.1.5.9. La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS

2.1.5.10. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL

2.1.5.11. Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente

2.1.5.12. 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.

2.1.5.13. Los portales personalizados deberán soportar al menos la definición de:

2.1.5.14. Widgets a mostrar

2.1.5.15. Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC

2.1.5.16. Esquema de colores

2.1.5.17. Soporte para Escritorio Virtual

2.1.5.18. Política de verificación de la estación de trabajo.

2.1.5.19. 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.

2.1.5.20. 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 autentificación nuevamente.

2.1.6.*Funcionalidades y Características del Sistema en Traffic Shapping / QoS*

2.1.6.1. Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall

2.1.6.2. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión

2.1.6.3. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.

2.1.6.4. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo

2.1.6.5. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo

2.1.6.6. Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia

2.1.7.*Funcionalidades y Características del Sistema en Autenticación y Certificación Digital*

2.1.7.1. Capacidad de integrarse con Servidores de Autenticación RADIUS.

2.1.7.2. Capacidad nativa de integrarse con directorios LDAP

2.1.7.3. 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”

2.1.7.4. 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.

2.1.7.5. Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.

2.1.7.6. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)

2.1.7.7. La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.

2.1.7.8. Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.

2.1.7.9. Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:

2.1.7.9.1. Longitud mínima permitida

2.1.7.9.2. Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.

2.1.7.9.3. Expiración de contraseña.

2.1.7.10. Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

2.1.8.*Funcionalidades y Características del Sistema en Antivirus*

2.1.8.1. 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.

2.1.8.2. 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.

2.1.8.3. 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.

2.1.8.4. El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.

2.1.8.5. 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.

2.1.8.6. 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.

2.1.8.7. El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos.

2.1.8.8. 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

2.1.8.9. 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.

2.1.8.10. 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.

2.1.8.11. El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.

2.1.8.12. El antivirus deberá ser capaz de filtrar archivos por extensión

2.1.8.13. El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables, por ejemplo) sin importar la extensión que tenga el archivo

2.1.8.14. 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)

2.1.9.*Funcionalidades y Características del Sistema en AntiSpam*

2.1.9.1. La capacidad antispam incluída 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.

2.1.9.2. La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).

2.1.9.3. 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

2.1.9.4. 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.

2.1.10. *Funcionalidades y Características del Sistema en Filtraje de URLs (URL Filtering)*

2.1.10.1. 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.

2.1.10.2. Debe poder categorizar contenido Web requerido mediante IPv6.

2.1.10.3. 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.

2.1.10.4. Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.

2.1.10.5. 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

2.1.10.6. 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).

2.1.10.7. 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.

2.1.10.8. Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido.

2.1.10.9. Capacidad de filtrado de scripts en páginas web (JAVA/Active X).

2.1.10.10. 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.

2.1.10.11. Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.

2.1.10.12. Será posible exceptuar la inspección de HTTPS por categoría.

2.1.10.13. 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.

2.1.10.13.1. El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección:

2.1.10.13.2. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.

2.1.10.13.3. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.

2.1.10.13.4. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado.

2.1.10.14. Se debe incluir la funcionalidad de reputación basada en filtrado de URLs.

2.1.10.15. La funcionalidad de reputación busca que, al acceder a páginas 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 página 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 zombis dentro de la red.

2.1.10.16. El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.

2.1.10.17. Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)

2.1.10.18. 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.

2.1.11. ***Funcionalidades y Características del Sistema en Protección contra intrusos (IPS)***

2.1.11.1. 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.

2.1.11.2. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.

2.1.11.3. Capacidad de detección de más de 4000 ataques.

2.1.11.4. 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)

2.1.11.5. 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.

2.1.11.6. 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).

2.1.11.7. Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.

2.1.11.8. Actualización automática de firmas para el detector de intrusos

2.1.11.9. El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.

2.1.11.10. Métodos de notificación:

2.1.11.10.1. Alarmas mostradas en la consola de administración del appliance.

2.1.11.10.2. Alertas vía correo electrónico.

2.1.11.11. 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.

2.1.11.12. 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.

2.1.11.13. 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.

2.1.11.14. Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir:

2.1.11.14.1. 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.

2.1.11.14.2. 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.

2.1.12. *Funcionalidades y Características del Sistema en Prevención de Fuga de Información (DLP)*

2.1.12.1. 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.

2.1.12.2. La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.

2.1.12.3. Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.

2.1.12.4. 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,

2.1.12.5. 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.

2.1.12.6. 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.

2.1.12.7. La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.

2.1.12.8. Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes:

2.1.12.8.1. Filtrado por tipo de archivo

2.1.12.8.2. Filtrado por nombre de archivo

2.1.12.8.3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.

2.1.12.9. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.

2.1.12.10. 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.

2.1.13. *Funcionalidades y Características del Sistema en Control de Aplicaciones*

2.1.13.1. Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.

2.1.13.2. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

2.1.13.3. La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.

2.1.13.4. El listado de aplicaciones debe actualizarse periódicamente.

2.1.13.5. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.

2.1.13.6. Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.

2.1.13.7. Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.

2.1.13.8. Preferentemente deben soportar mayor granularidad en las acciones.

2.1.14. *Funcionalidades y Características del Sistema en Inspección de Contenido SSL*

2.1.14.1. 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.

2.1.14.2. La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).

2.1.14.3. La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.

2.1.14.4. 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.

2.1.14.5. 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

2.1.15. *Funcionalidades y Características del Sistema en Controlador Inalámbrico (Wireless Controller)*

2.1.15.1. El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless

2.1.15.2. 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.

2.1.15.3. Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection.

2.1.15.4. 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.

2.1.15.5. Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.

2.1.15.6. La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión.

2.1.15.7. 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.

2.1.15.8. 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.

2.1.15.9. 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.

2.1.15.10. Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred.

2.1.15.11. 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)

2.1.15.12. El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota.

2.1.15.13. 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.

2.1.15.14. El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red.

2.1.15.15. 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,

2.1.15.16. 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

2.1.15.17. 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, Laptoos, PCs (tanto en Windows como en Linux)

2.1.15.18. 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.

2.1.16. ***Funcionalidades y Características del Sistema en Filtraje de tráfico VoIP, Peer-to-Peer y Mensajería instantánea***

2.1.16.1. Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).

2.1.16.2. 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.

2.1.16.3. 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.

2.1.16.4. La solución debe contar con un ALG (Application Layer Gateway) de SIP

2.1.16.5. Debe poder hacerse inspección de encabezados de SIP

2.1.16.6. Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP.

2.1.16.7. La solución debe soportar SIP HNT (Hosted NAT Transversal).

2.1.16.8. La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes

2.1.16.9. Deberá ser capaz de hacer inspección tráifco SSH en modo proxy explicito

2.1.16.10. La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo

2.1.16.11. El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS

2.1.17. ***Funcionalidades y Características del Sistema en Alta Disponibilidad***

2.1.17.1. 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

2.1.17.2. Alta Disponibilidad en modo Activo-Pasivo

2.1.17.3. Alta Disponibilidad en modo Activo-Activo

2.1.17.4. Posibilidad de definir al menos dos interfaces para sincronía

2.1.17.5. El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red

2.1.17.6. Será posible definir interfaces de gestión independientes para cada miembro en un clúster.

2.1.18. ***Funcionalidades y Características del Sistema en Características de Administración***

2.1.18.1. Interface 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 interface debe soportar SSL sobre HTTP (HTTPS)

2.1.18.2. La interface gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.

2.1.18.3. Interface basada en línea de comando (CLI) para administración de la solución.

2.1.18.4. Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.

2.1.18.5. Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)

2.1.18.6. El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.

2.1.18.7. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.

2.1.18.8. 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.

2.1.18.9. 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.

2.1.18.10. Soporte de SNMP versión 2

2.1.18.11. Soporte de SNMP versión 3

2.1.18.12. Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos

2.1.18.13. Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.

2.1.18.14. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.

2.1.18.15. 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.

2.1.18.16. 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.

2.1.18.17. Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.

2.1.18.18. Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho.

2.1.18.19. Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).

2.1.18.20. 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.

2.1.18.21. Contar con herramientas gráficas 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.

2.1.19. *Funcionalidades y Características del Sistema en Virtualización*

2.1.19.1. El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”

2.1.19.2. La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus

2.1.19.3. Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.

2.1.19.4. Cada instancia virtual debe poder tener un administrador independiente

2.1.19.5. La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.

2.1.19.6. Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red

2.1.19.7. Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual

2.1.19.8. Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.

2.1.19.9. Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

2.1.19.10. Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico 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.

2.1.20. *Funcionalidades y Características del Sistema en Análisis de Seguridad y Almacenamiento de Logs en la Nube*

2.1.20.1. 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.

2.1.20.2. 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 legitimo o ilegitimo, por medio de técnicas de Caja de Arena o Sandboxing.

2.1.20.3. Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse.

2.1.20.4. Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz.

2.1.20.5. Permitir Monitoreo y alertas en tiempo real.

2.1.20.6. Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis.

2.1.20.7. 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.

2.1.21. *Actualizaciones de plataforma*

2.1.21.1. La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD

2.1.21.2. 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

2.1.21.3. 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

2.1.21.4. 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

2.1.22. *Licenciamiento y actualizaciones*

2.1.22.1. 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.

2.1.22.2. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos por doce (12) meses.

2.1.23. *Funcionalidades y Características del Sistema en Desempeño / Conectividad*

2.1.23.1. El equipo debe por lo menos ofrecer las características de desempeño y conectividad indicadas en el siguiente cuadro.

Puertos de Consola	1
Puertos USB	2
Puertos para Administración GE	2
Puertos RJ45 GE	8
GE Slots SFP	8
Slots 10 GE SFP+	2
Transceiver Incluidos	2 SFP SX
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	36/36/24 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	36/36/24 Gbps
Firewall Latency (64 byte, UDP)	3 µs
Firewall Throughput (Paquetes por Segundo)	36 Mpps
Sesiones Concurrentes	5.5 Million
Nuevas Sesiones por Segundo	270000
Políticas de Firewall	10000
IPsec VPN Throughput (512 byte)	20 Gbps
Túneles IPSEC Sitio a Sitio	2000
Túneles IPSEC Cliente a Sitio	10000
Túnel SSL Throughput	2.2 Gbps
Máximo de Usuarios Concurrentes para el Túnel SSL	5000
IPS Throughput (HTTP / Enterprise Mix	7/4 Gbps
SSL Inspection Throughput	3.5 Gbps
Application Control Throughput	6 Gbps
NGFW Throughput	3.2 Gbps
Threat Protection Throughput	2.4 Gbps
CAPWAP Throughput	10 Gbps
Instancias Virtuales	8
Configuración de Alta Disponibilidad	Activo-Activo/Activo-Pasivo
Dimensiones de Rack	1 RU
AC Power Supply	100–240V AC, 60–50 Hz
Fuentes Redundantes	Debe soportar FRPS-100
Peso	11.46 lbs (5.2 kg)
Certificaciones del Equipo	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

2.2. *Renglón Nº 2: Contratación de Equipo de Seguridad Informática Perimetral para Edificio Pedro Arias*

Se requiere gestionar la adquisición de una persona jurídica que brinde el suministro de un sistema de seguridad informática perimetral, del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés), con las siguientes características ***mínimas***:

2.2.1.*Funcionalidades y Características del Sistema en Características del dispositivo*

2.2.1.1. El dispositivo debe ser un equipo de propósito específico.

2.2.1.2. 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.

2.2.1.3. Capacidad de incrementar el rendimiento de VPN a través de soluciones en hardware dentro del mismo dispositivo (mediante el uso de un ASIC).

2.2.1.4. Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).

2.2.1.5. El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red.

2.2.1.6. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.

2.2.1.7. El sistema operativo debe incluir un servidor de DNS que permita resolver de forma local ciertas consultas de acuerdo a la configuración del administrador.

2.2.1.8. 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.

2.2.2.*Funcionalidades y Características del Sistema en Firewall*

2.2.2.1. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.

2.2.2.2. 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.

2.2.2.3. Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.

2.2.2.4. 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

2.2.2.5. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.

2.2.2.6. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo.

2.2.2.7. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)

2.2.2.8. Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.

2.2.2.9. Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP)

2.2.2.10. Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.

2.2.2.11. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.

2.2.2.12. 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),

2.2.2.13. 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.

2.2.2.14. En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID

2.2.2.15. 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.

2.2.2.16. 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.

2.2.2.17. 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

2.2.2.18. La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.

2.2.2.19. 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

2.2.2.20. La solución será capaz de integrar los servicios dentro de las categorías de Firewall predefinidas o personalizadas y ordenarlos alfabéticamente

2.2.2.21. El dispositivo de seguridad podrá determinar accesos y denegación a diferentes tipos de tráfico predefinidos dentro de una lista local de políticas

2.2.2.22. 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

2.2.2.23. 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

2.2.2.24. El dispositivo de seguridad será capaz de crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces.

2.2.2.25. El dispositivo de generar logs de cada una de las políticas aplicadas para evitar los ataques de DoS

2.2.2.26. La solución de seguridad permitirá configurar el mapeo de protocolos a puertos de manera global o especifica

2.2.2.27. La solución capaz de configurar el bloqueo de archivos o correos electrónicos por tamaño, o por certificados SSL inválidos.

2.2.2.28. El dispositivo integrara la inspección de tráfico tipo SSL y SSH bajo perfiles predefinidos o personalizados

2.2.2.29. El dispositivo será capaz de ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico

2.2.2.30. Tendrá la capacidad de hacer escaneo a profundidad de trafico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis

2.2.2.31. La solución permitirá bloquear o monitorear toda la actividad de tipo Exec, Port-Forward, SSH-Shell, y X-11 SSH

2.2.3.*Funcionalidades y Características del Sistema en Conectividad y Sistema de ruteo*

2.2.3.1. Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP.

2.2.3.2. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.

2.2.3.3. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.

2.2.3.4. Soporte a políticas de ruteo (policy routing).

2.2.3.5. 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

2.2.3.6. Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS

2.2.3.7. Soporte a ruteo dinámico RIPng, OSPFv3

2.2.3.8. La configuración de BGP debe soportar Autonomous System Path (AS-PATH) de 4 bytes.

2.2.3.9. Soporte de ECMP (Equal Cost Multi-Path)

2.2.3.10. 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.

2.2.3.11. 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.

2.2.3.12. Soporte a ruteo de multicast

2.2.3.13. La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.

2.2.3.14. La solución podrá habilitar políticas de ruteo en IPv6

2.2.3.15. La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6

2.2.3.16. 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

2.2.3.17. 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

2.2.3.18. El dispositivo debe integrar la autenticación por usuario o dispositivo en IPv6

2.2.3.19. El dispositivo deberá soportar la inspección de tráfico IPv6 en modo proxy explicito

2.2.3.20. Deberá ser capaz de integrar políticas con proxy explicito en IPv6

2.2.3.21. La solución podrá restringir direcciones IPv6 en modo proxy explicito

2.2.3.22. Deberá hacer NAT de la red en IPv6

2.2.3.23. La solución será capaz de comunicar direccionamiento IPv6 a servicios con IPv4 a través de NAT

2.2.3.24. Como dispositivo de seguridad deberá soportar la inspección de tráfico IPv6 basada en flujo

2.2.3.25. 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

2.2.3.26. La solución contara con una base de administración de información interna generada por sesiones sobre IPv6

2.2.3.27. Deberá ser capaz de habilitar la funcionalidad de Traffic Shaper por IP dentro de las políticas creadas en IPv6

2.2.3.28. El dispositivo podrá tener la capacidad de transmitir DHCP en IPv6

2.2.3.29. La solución tendrá la funcionalidad de habilitar DHCP en IPv6 por interface

2.2.3.30. La solución deberá contar con soporte para sincronizar por sesiones TCP en IPv6 entre dispositivos para intercambio de configuración en Alta Disponibilidad

2.2.3.31. El dispositivo podrá ser configurado mediante DHCP en IPv6 para comunicarse con un servidor TFTP donde se encontrará el archivo de configuración

2.2.3.32. El dispositivo podrá hacer la función como servidor DHCP IPv6

2.2.3.33. La solución será capaz de configurar la autenticación por usuario por interface en IPv6

2.2.4.*Funcionalidades y Características del Sistema en VPN IPSec / L2TP/PPTP*

2.2.4.1. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)

2.2.4.2. Soporte para IKEv2 y IKE Configuration Method

2.2.4.3. Debe soportar la configuración de túneles PPTP

2.2.4.4. Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.

2.2.4.5. Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits

2.2.4.6. Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.

2.2.4.7. Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.

2.2.4.8. Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.

2.2.4.9. La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)

2.2.4.10. 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.

2.2.4.11. Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.

2.2.5.*Funcionalidades y Características del Sistema en VPN SSL*

2.2.5.1. Capacidad de realizar SSL VPNs.

2.2.5.2. Soporte a certificados PKI X.509 para construcción de VPNs SSL.

2.2.5.3. 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.

2.2.5.4. Soporte de renovación de contraseñas para LDAP y RADIUS.

2.2.5.5. Soporte a asignación de aplicaciones permitidas por grupo de usuarios

2.2.5.6. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.

2.2.5.7. 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.

2.2.5.8. Capacidad integrada para eliminar y/o cifrar el contenido descargado al caché de la máquina cliente (caché cleaning)

2.2.5.9. La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS

2.2.5.10. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL

2.2.5.11. Deberá soportar la redirección de página http a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente

2.2.5.12. 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.

2.2.5.13. Los portales personalizados deberán soportar al menos la definición de:

2.2.5.13.1. Widgets a mostrar

2.2.5.13.2. Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC

2.2.5.13.3. Esquema de colores

2.2.5.13.4. Soporte para Escritorio Virtual

2.2.5.13.5. Política de verificación de la estación de trabajo.

2.2.5.14. 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.

2.2.5.15. 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 autentificación nuevamente.

2.2.6.*Funcionalidades y Características del Sistema en Traffic Shapping / QoS*

2.2.6.1. Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall

2.2.6.2. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión

2.2.6.3. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.

2.2.6.4. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo

2.2.6.5. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo

2.2.6.6. Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia

2.2.7.*Funcionalidades y Características del Sistema en Autenticación y Certificación Digital*

2.2.7.1. Capacidad de integrarse con Servidores de Autenticación RADIUS.

2.2.7.2. Capacidad nativa de integrarse con directorios LDAP

2.2.7.3. 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”

2.2.7.4. 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.

2.2.7.5. Debe ser posible definir puertos alternativos de autenticación para los protocolos http, FTP y Telnet.

2.2.7.6. Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)

2.2.7.7. La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.

2.2.7.8. Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.

2.2.7.9. Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:

2.2.7.9.1. Longitud mínima permitida

2.2.7.9.2. Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.

2.2.7.9.3. Expiración de contraseña.

2.2.7.10. Debe poder limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.

2.2.8.*Funcionalidades y Características del Sistema en Antivirus*

2.2.8.1. 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.

2.2.8.2. 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.

2.2.8.3. 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.

2.2.8.4. El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6.

2.2.8.5. 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.

2.2.8.6. 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.

2.2.8.7. El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos.

2.2.8.8. 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

2.2.8.9. 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.

2.2.8.10. 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.

2.2.8.11. El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.

2.2.8.12. El antivirus deberá ser capaz de filtrar archivos por extensión

2.2.8.13. El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables, por ejemplo) sin importar la extensión que tenga el archivo

2.2.8.14. 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)

2.2.9.*Funcionalidades y Características del Sistema en AntiSpam*

2.2.9.1. 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.

2.2.9.2. 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).

2.2.9.3. 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

2.2.9.4. 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.

2.2.10. *Funcionalidades y Características del Sistema en Filtraje de URLs (URL Filtering)*

2.2.10.1. 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.

2.2.10.2. Debe poder categorizar contenido Web requerido mediante IPv6.

2.2.10.3. 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.

2.2.10.4. Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.

2.2.10.5. 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

2.2.10.6. 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).

2.2.10.7. 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.

2.2.10.8. Los mensajes de remplazo deben poder ser personalizados por categoría de filtrado de contenido.

2.2.10.9. Capacidad de filtrado de scripts en páginas web (JAVA/Active X).

2.2.10.10. 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.

2.2.10.11. Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.

2.2.10.12. Será posible exceptuar la inspección de HTTPS por categoría.

2.2.10.13. 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.

2.2.10.14. El sistema de filtrado de URLs debe tener al menos 3 métodos de inspección:

2.2.10.14.1. Modo de Flujo: La página es inspeccionada paquete a paquete sin reconstruir la página completa.

2.2.10.14.2. Modo Proxy: La página es reconstruida completamente para ser analizada a profundidad.

2.2.10.14.3. Modo DNS: La inspección se basa únicamente en la categorización del dominio accesado.

2.2.10.15. Se debe incluir la funcionalidad de reputación basada en filtrado de URLs.

2.2.10.16. La funcionalidad de reputación busca que, al acceder a páginas 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 página 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 zombis dentro de la red.

2.2.10.17. El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.

2.2.10.18. Se debe incorporar la funcionalidad de filtrado educativo de Youtube (Youtube Education Filter)

2.2.10.19. 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.

2.2.11. ***Funcionalidades y Características del Sistema en Protección contra intrusos (IPS)***

2.2.11.1. 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.

2.2.11.2. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6. A través de sensores.

2.2.11.3. Capacidad de detección de más de 4000 ataques.

2.2.11.4. 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)

2.2.11.5. 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.

2.2.11.6. 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).

2.2.11.7. Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.

2.2.11.8. Actualización automática de firmas para el detector de intrusos

2.2.11.9. El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.

2.2.11.10. Métodos de notificación:

2.2.11.10.1. Alarmas mostradas en la consola de administración del appliance.

2.2.11.10.2. Alertas vía correo electrónico.

2.2.11.11. 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.

2.2.11.12. 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.

2.2.11.13. 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.

2.2.11.14. Se debe incluir protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats). Dentro de estos controles se debe incluir:

2.2.11.14.1. 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.

2.2.11.14.2. 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.

2.2.12. *Funcionalidades y Características del Sistema en Prevención de Fuga de Información (DLP)*

2.2.12.1. 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.

2.2.12.2. La funcionalidad debe soportar el análisis de archivos del tipo: MS-Word, PDF, Texto, Archivos comprimidos.

2.2.12.3. Debe soportarse el escaneo de archivos en al menos los siguientes protocolos: HTTP, POP3, SMTP, IMAP, NNTP y FTP.

2.2.12.4. 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,

2.2.12.5. 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.

2.2.12.6. 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.

2.2.12.7. La solución debe permitir la búsqueda de patrones en archivos mediante la definición de expresiones regulares.

2.2.12.8. Se debe proveer la funcionalidad de filtrado de fuga de información. Dentro de las técnicas de detección se debe considerar como mínimo las siguientes:

2.2.12.8.1. Filtrado por tipo de archivo

2.2.12.8.2. Filtrado por nombre de archivo

2.2.12.8.3. Filtrado por expresiones regulares: Se detectarán los archivos según las expresiones regulares que se encuentren dentro de los mismos.

2.2.12.8.4. Fingerprinting: Se tomará una muestra del archivo que se considere como confidencial. Según esto se bloquearán archivos que sean iguales a esta muestra.

2.2.12.8.5. 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.

2.2.13. *Funcionalidades y Características del Sistema en Control de Aplicaciones*

2.2.13.1. Lo solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.

2.2.13.2. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.

2.2.13.3. La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.

2.2.13.4. El listado de aplicaciones debe actualizarse periódicamente.

2.2.13.5. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.

2.2.13.6. Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.

2.2.13.7. Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.

2.2.13.8. Preferentemente deben soportar mayor granularidad en las acciones.

2.2.14. ***Funcionalidades y Características del Sistema en Inspección de Contenido SSL***

2.2.14.1. 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.

2.2.14.2. La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).

2.2.14.3. La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.

2.2.14.4. 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.

2.2.14.5. 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

2.2.15. ***Funcionalidades y Características del Sistema en Controlador Inalámbrico (Wireless Controller)***

2.2.16. El dispositivo debe tener la capacidad de funcionar como Controlador de Wireless

2.2.17. 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.

2.2.18. Debe soportar la funcionalidad de detección y mitigación de puntos de acceso (APs). Rogue Access Point Detection.

2.2.19. 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.

2.2.20. Deberá tener la capacidad de monitorear las estaciones de trabajo, clientes wireless, conectadas a alguno de los APs.

2.2.21. La solución debe contar con la funcionalidad de WIDS (Wireless IDS), la capacidad de monitorear el trafico wireless para detectar y reportar posibles intentos de intrusión.

2.2.22. 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.

2.2.23. 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.

2.2.24. 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.

2.2.25. Debe contar con la capacidad de realizar Bridge SSID, permitiendo que una red inalámbrica y un segmento cableado LAN pertenezcan a la misma rubred.

2.2.26. 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)

2.2.27. El dispositivo debe tener la capacidad de controlar varios puntos de acceso de la misma plataforma de forma remota.

2.2.28. 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.

2.2.29. El dispositivo debe permitir la administración y manejo tanto de redes cableadas como inalámbricos dentro del mismo segmento de red.

2.2.30. 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,

2.2.31. 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

2.2.32. 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, Laptoos, PCs (tanto en Windows como en Linux)

2.2.33. 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.

2.2.34. *Funcionalidades y Características del Sistema en Filtraje de tráfico VoIP, Peer-to-Peer y Mensajería instantánea*

2.2.34.1. Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).

2.2.34.2. 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.

2.2.34.3. 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.

2.2.34.4. La solución debe contar con un ALG (Application Layer Gateway) de SIP

2.2.34.5. Debe poder hacerse inspección de encabezados de SIP

2.2.34.6. Deben poder limitarse la cantidad de requerimientos SIP que se hacen por segundo. Esto debe poder definirse por cada método SIP.

2.2.34.7. La solución debe soportar SIP HNT (Hosted NAT Transversal).

2.2.34.8. La solución deberá integrar la inspección de tráfico basado en flujo utilizando un motor de IPS dentro del mismo dispositivo para escaneo de paquetes

2.2.34.9. Deberá ser capaz de hacer inspección tráifco SSH en modo proxy explicito

2.2.34.10. La solución de seguridad podrá hacer inspección de tráfico HTTP, HTTPS y FTP sobre HTTP en modalidad proxy explicito con las funcionalidades de IPS, Antivirus, Filtrado Web, Control de Aplicaciones y DLP, todo en un mismo dispositivo

2.2.34.11. El dispositivo tendrá la opción para configurar sus interfaces integradas en modo Sniffer con funcionalidades de Filtrado Web, Control de Aplicaciones, Antivirus e IPS

2.2.35. *Funcionalidades y Características del Sistema en Alta Disponibilidad*

2.2.35.1. 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

2.2.35.2. Alta Disponibilidad en modo Activo-Pasivo

2.2.35.3. Alta Disponibilidad en modo Activo-Activo

2.2.35.4. Posibilidad de definir al menos dos interfaces para sincronía

2.2.35.5. El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red

2.2.35.6. Será posible definir interfaces de gestión independientes para cada miembro en un clúster.

2.2.36. *Funcionalidades y Características del Sistema en Características de Administración*

2.2.36.1. Interface 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 interface debe soportar SSL sobre HTTP (HTTPS)

2.2.36.2. La interface gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.

2.2.36.3. Interface basada en línea de comando (CLI) para administración de la solución.

2.2.36.4. Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.

2.2.36.5. Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)

2.2.36.6. El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.

2.2.36.7. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.

2.2.36.8. 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.

2.2.36.9. 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.

2.2.36.10. Soporte de SNMP versión 2

2.2.36.11. Soporte de SNMP versión 3

2.2.36.12. Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos

2.2.36.13. Soporte para almacenamiento de eventos en un repositorio que pueda consultarse luego con SQL.

2.2.36.14. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.

2.2.36.15. 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.

2.2.36.16. 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.

2.2.36.17. Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.

2.2.36.18. Contar con facilidades de administración a través de la interfaz gráfica como listas de edición a través de click derecho.

2.2.36.19. Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).

2.2.36.20. 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.

2.2.36.21. Contar con herramientas gráficas 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.

2.2.37. *Funcionalidades y Características del Sistema en Virtualización*

2.2.37.1. El dispositivo deberá poder virtualizar los servicios de seguridad mediante “Virtual Systems”, “Virtual Firewalls” o “Virtual Domains”

2.2.37.2. La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus

2.2.37.3. Se debe incluir la licencia para al menos 8 (ocho) instancias virtuales dentro de la solución a proveer.

2.2.37.4. Cada instancia virtual debe poder tener un administrador independiente

2.2.37.5. La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.

2.2.37.6. Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red

2.2.37.7. Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual

2.2.37.8. Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.

2.2.37.9. Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual.

2.2.37.10. Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico 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.

2.2.38. ***Funcionalidades y Características del Sistema en Análisis de Seguridad y Almacenamiento de Logs en la Nube***

2.2.38.1. 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.

2.2.38.2. 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 legitimo o ilegitimo, por medio de técnicas de Caja de Arena o Sandboxing.

2.2.38.3. Almacenamiento de Logs hasta 1 Giga por equipo incluido con capacidad de crecimiento en caso de requerirse.

2.2.38.4. Debe permitir administración centralizada de todos los equipos de la solución de seguridad perimetral desde una misma interfaz.

2.2.38.5. Permitir Monitoreo y alertas en tiempo real.

2.2.38.6. Debe contar con Reportes predefinidos y la opción de personalización, así como contar con herramientas de análisis.

2.2.38.7. 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.

2.2.39. *Actualizaciones de plataforma*

2.2.39.1. La solución contara con el servicio de actualización de firmas para dispositivos sobre BYOD

2.2.39.2. 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

2.2.39.3. 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

2.2.39.4. 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

2.2.40. *Licenciamiento y actualizaciones*

2.2.40.1. 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.

2.2.40.2. La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos doce (12) meses.

2.2.41. *Funcionalidades y Características del Sistema en Desempeño / Conectividad*

2.2.41.1. El equipo debe por lo menos ofrecer las características de desempeño y conectividad indicadas en el siguiente cuadro.

Puertos de Consola	1
Puertos USB	2
Puertos para Administración GE	1
Puertos RJ45 GE	16
GE Slots SFP	2
Slots 10 GE SFP+	0
Transceiver Incluidos	0
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	2.3 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	2.3 Gbps
Firewall Latency (64 byte, UDP)	37 µs
Sesiones Concurrentes	2.5 Million
Nuevas Sesiones por Segundo	20.000
Políticas de Firewall	8.000
IPsec VPN Throughput (512 byte)	450 Mbps
Túneles IPSEC Sitio a Sitio	1.000
Túneles IPSEC Cliente a Sitio	2.000
Túnel SSL Throughput	250 Mbps
Máximo de Usuarios Concurrentes para el Túnel SSL	250
IPS Throughput (HTTP / Enterprise Mix	500/300 Mbps
SSL Inspection Throughput	250 Mbps
Application Control Throughput	300 Mbps
NGFW Throughput	200 Mbps
Threat Protection Throughput	200 Mbps
CAPWAP Throughput	1 Gbps
Instancias Virtuales	8
Configuración de Alta Disponibilidad	Activo-Activo/Activo-Pasivo
Dimensiones de Rack	1 RU
AC Power Supply	100–240V AC, 60–50 Hz
Peso	9.5 lbs (4.3 kg)
Certificaciones del Equipo	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6

2.3. *Renglón Nº 3: Appliance para Consolidación de Logs y Administración de Reportes*

Se requiere gestionar la adquisición de una persona jurídica que brinde el suministro 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), con las siguientes características ***mínimas***:

2.3.1.*Funcionalidades y Características del Sistema del dispositivo*

2.3.1.1. Sistema de Almacenamiento de Logs y Reportes.

2.3.1.2. Dispositivo tipo appliance de propósito específico, el cual también debe contar con la posibilidad de implementarse sobre ambientes virtuales.

2.3.1.3. Sistema operativo propietario

2.3.1.4. Interface de administración gráfica (GUI) vía Web (HTTPS)

2.3.1.5. Interface de administración vía CLI (Línea de comando), vía ssh y consola serial

2.3.1.6. Permite la definición de dominios administrativos independientes para dividir o segmentar el control de la información recibida y almacenada por dispositivo.

2.3.1.7. Tiene la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas

2.3.1.8. Permite la posibilidad de utilizar repositorio de datos externos (bases de datos)

2.3.1.9. Permite integrar dispositivos para que reporten, y establezcan comunicaciones seguras con dichos dispositivos

2.3.1.10. Permite asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución

2.3.1.11. 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.

2.3.2.*Funcionalidades y Características del Sistema en Generación de reportes:*

2.3.2.1. Permite generar reportes personalizados, permite al administrador de la solución el determinar el contenido de los reportes.

2.3.2.2. El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart)

2.3.2.3. Genera reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.

2.3.2.4. Genera reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.

2.3.2.5. Genera reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.

2.3.2.6. Permite de generar la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino.

2.3.2.7. Permite generar un reporte de las actividades administrativas (entradas de administradores, cambios de configuración) realizadas.

2.3.2.8. Permite personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana.

2.3.2.9. 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).

2.3.2.10. Permite la calendarización de reportes.

2.3.2.11. Permite generar reportes en formato PDF y DOC.

2.3.2.12. Debe tener la opción de generar reportes en idioma inglés y en idioma español

2.3.2.13. Debe permite enviar el reporte vía correo electrónico.

2.3.3. *Funcionalidades y Características del Sistema en Análisis forense y correlación:*

2.3.3.1. 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.

2.3.4.*Funcionalidades y Características del Sistema en Almacenamiento de Contenido:*

2.3.4.1. 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

2.3.4.2. 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.

2.3.4.3. Permite hacer búsquedas sobre los mensajes almacenados

2.3.5.*Funcionalidades y Características del Sistema en Otras Consideraciones*

2.3.5.1. Requisitos para VMware

2.3.5.1.1. GB / Logs por día +1

2.3.5.1.2. Capacidad de Almacenamiento +500GB

2.3.5.1.3. Dispositivos / ADOMs / VDOMs Compatibles (Máximo) 10,000

2.3.5.2. Requisitos de admisibilidad

2.3.5.2.1. El oferente debe incluir en su propuesta la carta de exportación del producto la cual es requisito indispensable para instituciones de Gobierno.

2.3.5.2.2. Toda la solución debe venir acompañada con 10 dispositivos de acceso de doble autentificación o Token, por medio VPN SSL.

3. REQUERIMIENTOS TÉCNICOS

3.1. ***Plazo de ejecución:*** Los servicios deben ejecutarse en un plazo cuatro (4) meses contados a partir de la recepción de la orden de inicio por parte el Proceso Informática, la cual se emitirá luego de otorgado el refrendo del contrato por el área competente. Quién indique en la oferta un plazo fuera del rango solicitado no será sujeto de análisis y se procederá a la exclusión de la misma.

3.2. ***Seguridad***

3.2.1. El oferente debe comprometerse a cumplir con las disposiciones Seguridad Informática establecidas por las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República e implementar la solución ofertada tomando en consideración las Políticas de Seguridad Informática establecidas por y para la Municipalidad de Escazú., mismas que podrán ser revisadas por el Proceso de Informática, sin opción de sacar copia de dichos documentos.

3.2.2. De los aspectos de seguridad citados en esta sección, según las disposiciones establecidas por las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de la República, deben observarse los que apliquen a los servicios requeridos (hardware y software). Aquellas condiciones que el oferente estime no aplican al objeto de esta contratación, deben indicarse las razones por las que se consideran no aplicables. Para este último caso, la Municipalidad se reserva la potestad de no aceptar dichas ofertas.

3.2.3. Para las herramientas de administración y monitoreo de los componentes de la solución, el oferente debe garantizar que éstas utilizan ambientes y canales seguros, que únicamente se habilitan los servicios y puertos estrictamente requeridos para que las herramientas funcionen. No deben existir mecanismos alternos para administrar o monitorear los componentes de la solución. Toda la configuración necesaria para el uso de estas herramientas debe ser documentada y entregada junto con la solución.

3.2.4. El sistema deberá generar copias de seguridad automáticas para garantizar la salvaguarda y conservación de los datos.

3.2.5. El sistema deberá tener todos los atributos de seguridad procedimental, de propiedad, confidencialidad, privacidad, de integridad y exactitud tanto de la base de datos como de los módulos que componen el sistema.

3.2.6. El oferente podrá emitir recomendaciones adicionales sobre la seguridad en la cual correrá el aplicativo. Para aquellas recomendaciones que impliquen un costo, deberá cotizar de manera independiente.

3.2.7. El oferente debe comprometerse, en caso de resultar adjudicado, a que facilitará la documentación técnica necesaria sobre el modelo o esquema de Seguridad utilizado por el aplicativo.

3.2.8. El oferente garantizará, dentro de su ámbito de competencia, la integridad y seguridad de la información almacenada en el aplicativo.

3.2.9. El oferente garantiza que la solución no incluye funcionalidades no solicitadas en el cartel que puedan afectar la operación de la Municipalidad de Escazú, ya sea en forma de estafa, sabotaje u otro acto de carácter doloso.

3.2.10. El oferente acepta que la Municipalidad de Escazú pueda aplicar procesos de revisión, hardening y de prueba de penetraciones, para poder dar visto bueno a la puesta en operación del sistema.

3.3. *Configuración*

3.3.1. El sistema deberá ser lo suficientemente flexible para adaptarse a cambios en el entorno, en los procedimientos y permitir cambiar la configuración de manera rápida y efectiva (parametrización) sin que ello afecte la funcionalidad del producto terminado.

3.3.2. Las pantallas en general, así como los mensajes de errores se mostrarán en español y deben ser los suficientemente claros como para determinar la causa del error y las acciones correctivas.

3.3.3. El oferente debe informar, en caso de resultar adjudicado, las configuraciones del sistema que están de manera predeterminada y permitir ajustes a dicha configuración previo acuerdo entre las partes.

3.4. ***Instalación y operación***

3.4.1. El sistema debe poder instalarse y operar sin problema alguno como mínimo en plataformas de hardware con arquitectura de treinta y dos (32) bits y sesenta y cuatro (64) bits.

3.4.2. El oferente deberá configurar en su totalidad los equipos ofertados, en cada uno de las funcionalidades solicitadas en los reglones 1,2 y 3.

3.4.3. El sistema deberá poder instalarse y ejecutarse a nivel de cliente o estación de trabajo de los usuarios con el sistema operativo Microsoft Windows XP, 7, 8, 8.1 y 10 o versión superior de Microsoft Windows o en su efecto en plataformas de VMWare.

3.4.4. La instalación la debe realizar un experto en los equipos ofertados para lo cual deberá estar certificado a nivel medio o 3 de la marca, para lo que deberá aportar copia de títulos o certificados que lo acrediten.

3.4.5. Para la implementación de todos y cada uno de los componentes de la solución el oferente deberá efectuar la instalación y configuración de estos tomando en cuenta las mejores prácticas de seguridad establecidas por el fabricante del componente y/o en ausencia de dichas prácticas, las recomendadas por la Industria. En este sentido, las consideraciones de seguridad deben ser tomadas en cuenta desde la instalación de los componentes de la solución, el software que requiera de niveles de autorización deberá ser configurado en primera instancia bajo el principio del “menor privilegio posible”.

3.4.6. El oferente debe proveer todo programa utilitario o software y su respectivo licenciamiento para que la aplicación funcione correctamente.

4. GARANTÍA DE FUNCIONAMIENTO

4.1. Todos los equipos solicitados deberán tener una garantía mínima de un año, con posibilidad de extensión de la misma.

4.2. De igual manera debe ser incluida en la oferta la subscripción por 12 meses de todas las licencias de los mismos.

4.3. La garantía deberá comprender, como mínimo, los defectos de fabricación, instalación, componentes y funcionamiento. Se entiende que durante el período de garantía los costos de mantenimiento (mano de obra, repuestos y todo otro requerimiento) preventivo y correctivo correrán por cuenta del proveedor.

4.4. Los equipos deben ser nuevos y no re manufacturados.

5. CONDICIONES ESENCIALES DEL SERVICIO DE CAPACITACIÓN

5.1. El oferente deberá brindar una capacitación a un mínimo de dos (2) personas, con una duración minino de dieciséis (16) horas, como parte del proceso de implementación de los productos ofertados.

5.2. La prestación del servicio de capacitación no originará relación de empleo público entre la Administración y la persona jurídica adjudicada; por lo que los costos originados por concepto de cargas sociales y seguros correrán por cuenta del adjudicado, ya sea persona jurídica.

5.3. La persona jurídica adjudicada deberá presentar, al Proceso Informática, el plan de trabajo y metodología del servicio de capacitación, que debe ser teórico - práctico, contar con dinámicas y actividades que permitan a las personas participantes aplicar sus conocimientos en forma paralela, y así evacuar las dudas que surjan como parte del proceso.

5.4. La capacitación debe ser al menos 25% teórico y 75% práctico.

5.5. Dicho programa del servicio de capacitación debe cumplir como ***mínimo*** con lo siguiente:

5.5.1. La persona jurídica oferente garantizará la ejecución de las actividades de capacitación necesarias para asegurar la transferencia de conocimiento a los funcionarios del Proceso Informática, en la utilización del sistema.

5.5.2. La persona jurídica adjudicada deberá indicar por escrito al Proceso de Informática en el plazo de diez (10) días hábiles, contados a partir del comunicado de firmeza del concurso, las fechas estimadas, horarios y temas de la capacitación, detallados por sesiones y horas de aprovechamiento.

5.5.3. La capacitación deberá coordinarse con el Proceso de Informática.

5.5.4. Todas las sesiones de capacitación deberán contar con material de apoyo, y el mismo deberá estar en idioma español y su costo debe estar incluido en el total de la oferta.

5.6. El instructor ofrecido deberá tener experiencia positiva impartiendo este tipo de capacitaciones con mínimo un año, para instituciones públicas o privadas.

5.7. Al finalizar cada curso se deberá entregar al Proceso de Recursos Humanos un listado de las personas que asistieron a la capacitación, firmada por la persona instructora.

5.8. La persona jurídica deberá para los cursos impartidos en dos (2) medios días brindar un refrigerio en la mañana, un almuerzo y un refrigerio en la tarde, para los cursos que consuman medio día se debe brindar un refrigerio.

5.9. ***Material Didáctico***

5.9.1. Debe estar en español.

5.9.2. La logística y costo del mismo correrá por parte de la persona jurídica adjudicada.

5.9.3. El programa del servicio de capacitación debe presentarse al Proceso de Informática tres (3) días hábiles antes del inicio de las actividades, delimitando los objetivos, temario a emplear.

5.9.4. La persona jurídica adjudicada deberá entregar a cada participante, el día de inicio del servicio de capacitación, el material didáctico relacionado con lo expuesto en el servicio de capacitación.

5.9.5. Deberá entregarse una (1) copia en disco compacto, una (1) copia escrita del material de la capacitación al Proceso de Informática del programa de capacitación. Dicho material debe presentarse ante el Proceso de Informática tres (3) días hábiles antes del inicio de las actividades.

5.9.6. En caso de que el material didáctico escrito, sea una reproducción o fotocopia, deberá cumplir con los estándares de calidad aplicables a la legibilidad de la palabra escrita, a las figuras, gráficos, o cualquier otra ilustración necesaria para esclarecer el contenido escrito.

5.10.*Equipos Didácticos*

5.10.1. La persona jurídica adjudicada deberá aportar los equipos didácticos necesarios que contribuyan al logro de los objetivos del servicio de capacitación.

5.10.2. Corresponderá a la persona jurídica adjudicada tramitar y pagar todo lo correspondiente al mantenimiento y uso del equipo didáctico necesario para brindar el servicio de capacitación.

5.10.3. La persona jurídica adjudicada deberá incluir como mínimo una computadora portátil y un video proyector para impartir las lecciones teóricas.

5.11.*Currículum*

5.11.1. Presentar currículum del instructor, donde resuma aspectos ***mínimos*** como:

5.11.1.1. Datos personales (nombre completo, nacionalidad, etc.)

5.11.1.2. Estudios realizados,

5.11.1.3. Experiencia laboral,

5.11.1.4. Otros estudios realizados.

5.11.2. El profesional que impartirá la capacitación debe contar con experiencia positiva mínima de tres (3) capacitaciones referentes a la operación de los dispositivos de seguridad requeridos por el cartel. Demostrable mediante una lista de referencia en la cual se aporte lista de referencia, con teléfonos y contactos para fines de verificación.

La información solicitada debe presentarse con el siguiente formato:

Persona Contacto	Empresa	Descripción Proyecto	Fecha Inicio (dd/mm/aaaa)	Fecha Final (dd/mm/aaaa)	Teléfono

La tabla de referencia será verificada por el área técnica.

5.11.3. El Proceso Informática se reserva el derecho de solicitar el reemplazo del instructor (es), si se considera que no cumple con los requerimientos solicitados.

5.12.*Lugar*

5.12.1. La capacitación se deberá realizar en las instalaciones de la Municipalidad de Escazú

6. EJECUCIÓN CONTRACTUAL

6.1. Implementación

6.1.1. La persona jurídica adjudicada deberá entregar al Proceso de Informática en el plazo de diez (10) días hábiles, contados a partir del comunicado de firmeza del concurso, un cronograma con actividades, fechas de inicio y fin estimados, técnicos responsables y entregables, para la instalación y operación del aplicativo, en concordancia con el Plazo de Entrega al que se comprometió. Dentro de dicho cronograma se deberá considerar:

6.1.1.1. Una semana para que el Proceso de Informática de la Municipalidad de Escazú realicen las pruebas que estime necesarias a la seguridad del aplicativo.

6.1.1.2. Una semana para realizar una revisión general de las características de los equipos del Proceso de Informática en los que se instalarán las licencias, e informar al Proceso de Informática en caso de requerirse algún elemento adicional de hardware o dispositivo periférico, con el propósito de asegurar una óptima instalación y operación del sistema.

6.1.1.3. Como parte de la revisión, realizar las recomendaciones que estime pertinentes, respecto las características de los equipos del Proceso de Informática, en los que se instalará el software, de la Municipalidad de Escazú, para asegurar la mayor confiabilidad, integridad y disponibilidad de la información.

6.1.1.4. Las pruebas que se requieran y las que solicite el Proceso Informática de la Municipalidad de Escazú, para verificar el fiel funcionamiento del software.

6.1.1.5. Colaborar con el Proceso Informática de la Municipalidad de Escazú para realizar una carga inicial y las pruebas de funcionalidad, con al menos diez (10) evaluaciones.

6.1.2. La persona jurídica adjudicada para la implementación deberá facilitar los técnicos necesarios para que trabajen concurrentemente, según el cronograma de actividades.

6.1.3. El Proceso de Informática dispondrá de cinco (5) días hábiles para hacer las observaciones que estime pertinente a la implementación, la persona jurídica adjudicada tendrá cinco (5) días hábiles para realizar y notificar los ajustes correspondientes.

6.1.4. La instalación iniciará cuando el Proceso de Informática notifique a la persona jurídica adjudicada la orden de inicio de la instalación.

6.1.5. El sistema deberá quedar debidamente instalado y operando correctamente en los equipos designados por el Proceso Informática, de modo que la Municipalidad de Escazú no tenga que incurrir en gastos, ni modificaciones adicionales para su correcta operación.

6.1.6. La persona jurídica adjudicada para la correcta instalación del software debe considerar la entrega e instalación del software debe realizarse en el Proceso Informática de la Municipalidad de Escazú, ubicada en el Palacio Municipal, costado norte del parque central de Escazú.

6.2. Mantenimiento y soporte

6.2.1. La persona jurídica oferente deberá indicar en su oferta un medio para realizar reportes, donde se pueda registrar los incidentes y darles seguimiento de su atención. Además, deberá indicar un correo electrónico, donde pueda establecerse comunicación oficial para la atención de incidentes o requerimientos varios que puedan surgir en la prestación de servicios.

6.2.2. La persona jurídica oferente se obliga a brindar a la Municipalidad de Escazú el servicio de mantenimiento y soporte que esta le solicite a raíz de un evento notificado y durante un plazo mínimo de doce (12) meses, a partir de que la Municipalidad de Escazú le entregue a la persona jurídica adjudicada la copia del contrato aprobado y el Proceso de Informática haya recibido a satisfacción la instalación y puesta en producción del software.

6.2.3. La persona jurídica oferente se obliga a brindar dentro del soporte al menos, la atención de errores del sistema, consultas de usuario, análisis de casos de usuarios por un total de 15 horas de servicio durante el periodo de los 12 meses.

6.2.4. La persona jurídica adjudicada se obliga a tener técnicos capacitados y disponibles, para la atención de cualquier incidente.

6.2.5. La persona jurídica adjudicada acepta en caso de desplazamiento físico de los equipos designados por el Proceso de Informática incluidas en esta contratación, instalar sin costo adicional el software en el equipo respectivo y dejarlo en correcto funcionamiento.

6.2.6. La persona jurídica adjudicada se compromete a que el tiempo de respuesta máximo para la resolución de fallas del sistema instalado (entiéndase como aquellas características funcionales y técnicas del sistema, especificadas en la oferta y que en algún momento de su operación fallaron) será de ocho (8) horas, en horario de 8:00 am a 4:00 pm. Dicho tiempo rige a partir de la comunicación del fallo, hasta la atención del reporte correspondiente.

7. RECEPCIÓN PROVISIONAL Y DEFINITIVA

7.1. La recepción provisional del objeto se regirá por lo establecido en el Artículo Nº 194 del Reglamento a la Ley de Contratación Administrativa y se entenderá como el recibo material del bien, por parte de del Proceso Informática. Para ello la persona jurídica adjudicada deberá coordinar con el Proceso Informática, la hora y demás condiciones necesarias para la recepción, cuando sea pertinente, o bien informar cuando se ha procedido con la entrega.

7.2. La recepción definitiva del objeto se regirá por lo establecido en el Artículo Nº 195 del Reglamento a la Ley de Contratación Administrativa y será extendida dentro del mes siguiente a la recepción provisional o dentro del plazo establecido en la primera página de la invitación, o bien vencido el plazo para corregir defectos. La recepción definitiva no excluye la aplicación de multa, si el servicio presenta alguna inconformidad con lo establecido en la orden de compra.

8. CONDICIONES DE ENTREGA

8.1. Debe entenderse que los productos a adquirir deben entregarse en las instalaciones de la Municipalidad de Escazú, según lo indicado por el Proceso Informática de la Municipalidad de Escazú.

8.2. De ser rendida la recepción definitiva del pedido, el funcionario del área solicitante rendirá el "recibido conforme" de la mercadería, por lo cual la persona jurídica adjudicada deberá cerciorarse de que junto con la firma de aceptación, se adicione la fecha en que se recibió la mercadería y se disponga del sello de la dependencia respectiva, el cumplimiento de dichos requisitos será obligatorio como parte de la gestión para tramitar el pago respectivo, caso que la factura no cuente con la globalidad de lo señalado, se estará posponiendo su cancelación hasta que se cumpla con la totalidad de las condiciones antes indicadas.

8.3. La lista de entrega y factura, que debe proporcionar la persona jurídica adjudicada, deberá especificar como mínimo: código de artículo, número de solicitud de suministros, descripción del artículo, cantidad solicitada, cantidad entregada, costo unitario y total, fecha de entrega y espacio para que el funcionario designado por la Municipalidad de Escazú consigne: Nombre, firma, fecha efectiva de recepción del producto y sello de la oficina.

8.4. Si el pedido es rechazado parcial o totalmente por errores imputables a la persona jurídica adjudicada, ésta deberá reponer lo respectivo en un período máximo de un día hábil después de la fecha del rechazo, asumiendo los costos de reposición, que de ninguna forma podrán ser trasladados a la Municipalidad de Escazú. Por otro lado, si los suministros consignados en la lista de entrega no corresponden en forma total o parcial a lo efectivamente entregado, el representante de la Municipalidad de Escazú, deberá indicarlo en dicha lista, en un espacio designado para este fin, anotándose código, cantidad y descripción de los productos rechazados o no recibidos.

8.5. Si durante el proceso de verificación se comprueba, que los bienes entregados por la persona jurídica adjudicada no cumplen con las características técnicas definidas, esté deberá retirar aquellos que no se ajusten o cumplan, debiendo reponerlos por otros que atiendan lo establecido, para lo cual tendrá un plazo máximo de un día hábil después de que reciba la debida comunicación por parte de la Municipalidad de Escazú.

8.6. Los costos de la reposición deberán ser asumidos íntegramente por la persona jurídica adjudicada, sin que puedan ser trasladados de forma alguna a la Municipalidad de Escazú.

8.7. En todo caso se aclara, que la persona jurídica adjudicada será enteramente responsable por los bienes, hasta tanto estos no hayan sido recibidos “a entera satisfacción” por la Municipalidad de Escazú.

8.8. Siempre y cuando que los bienes que se encuentren en buen estado de presentación, conservación, empaque y funcionamiento y cumplan con las calidades, características y condiciones establecidas en este cartel, serán aceptadas de conformidad por la Municipalidad de Escazú.

9. CONSIDERACIONES

9.1. La persona jurídica oferente debe adjuntar copia de título de al menos un técnico de la persona jurídica adjudicada, certificado por la marca del fabricante del producto cotizado. El mismo deberá contar con al menos tres (3) años de Certificado (a demostrar con el título solicitado) y se encargará principalmente de la cuenta y los casos de soporte requeridos por la Municipalidad

9.2. La Municipalidad de Escazú, según lo indicado en el Artículo N° 197 del Reglamento a la Ley de Contratación Administrativa la Administración, recibirá bienes actualizados cumpliendo con las siguientes reglas:

9.2.1. Que se trate de objetos de igual naturaleza y funcionalidad, con condiciones similares de instalación y mantenimiento.

9.2.2. Que el cambio constituya una mejora para la Administración, de frente a sus necesidades.

9.2.3. Que no se trate de actualizaciones que se encuentren en fase de investigación o que no hayan sido lo suficientemente probadas o carezcan de los respaldos pedidos en el cartel.

9.2.4. Que las condiciones restantes se mantengan inalteradas.

9.2.5. La última actualización se entenderá, entre otras cosas, como que el bien esté en línea de producción al momento de la entrega, o como la última versión del fabricante, cuando el objeto admita actualizaciones de esa naturaleza y ésta haya sido conocida en el mercado al menos un mes antes de la entrega de la orden de inicio. Para estos efectos, el oferente deberá respaldar el ofrecimiento con certificación emitida directamente por el fabricante.

9.2.6. La mejora deberá informarse por escrito, explicando en detalle en qué consiste el cambio, de ser necesario a partir de literatura técnica y cualesquiera otros elementos que resulten pertinentes.

9.2.7. Bajo ninguna circunstancia, los cambios en los bienes o servicios podrán desmeritar las garantías y condiciones de los bienes inicialmente ofrecidas, las cuales se consideran un mínimo que no podrá ser rebajado ante modificaciones de esta naturaleza.

10. RECIBO DEL OBJETO DE LA CONTRATACIÓN ACTUALIZADO

10.1. La persona jurídica adjudicada deberá entregar servicio adjudicado en las mejores condiciones y actualizados, todo ello considerando los dispuesto en el Artículo Nº 197 del Reglamento a la Ley de Contratación Administrativa, por lo que la Municipalidad de Escazú por medio del Proceso Informática estará facultado para aceptar las mejoras y cambios e innovaciones tecnológicas en los servicios que le proponga la persona jurídica adjudicada a su ofrecimiento y que se planteen con posterioridad a la apertura de las ofertas y aún en la fase de ejecución contractual, siempre que sea presentada por escrito, no le representen ningún costo adicional y que se reviertan a favor del mejor beneficio para la Municipalidad de Escazú medido en función de incrementos en la capacidad, calidad o potencialidad del objeto contratado. La persona jurídica adjudicada deberá soportar la solicitud con los documentos técnicos probatorios que respalden su gestión.

10.2. Previo a la aceptación de tales mejoras, el Proceso Informática procurará del área usuaria a cuyo encargo se promovió el procedimiento de contratación, las verificaciones y validaciones del caso que sustenten la aceptación de la mejora.

10.3. Estas mejoras no serán tomadas en cuenta en la valoración y comparación de la propuesta, pero obligarán a quienes las formulen una vez firme la adjudicación. Si la propuesta de mejora se realiza en la etapa de ejecución contractual, será obligación de la persona jurídica adjudicada suplir el bien o servicios bajo las nuevas condiciones pactadas.

10.4. La Municipalidad de Escazú contará con diez (10) días hábiles para la resolución de la solicitud y se tendrá por suspendido el plazo de entrega con la presentación de la gestión. Sin embargo, en el momento que la Municipalidad de Escazú considere que la documentación es insuficiente, se tendrá por activado el plazo de entrega hasta tanto la persona jurídica adjudicada no conteste la prevención que la Municipalidad de Escazú le remita.

10.5. La Municipalidad de Escazú, según lo indicado en el Artículo N° 197 del Reglamento a la Ley de Contratación Administrativa la Administración, recibirá bienes actualizados cumpliendo con las siguientes reglas:

10.5.1. Que se trate de objetos de igual naturaleza y funcionalidad, con condiciones similares de instalación y mantenimiento.

10.5.2. Que el cambio constituya una mejora para la Administración, de frente a sus necesidades.

10.5.3. Que no se trate de actualizaciones que se encuentren en fase de investigación o que no hayan sido lo suficientemente probadas o carezcan de los respaldos pedidos en el cartel.

10.5.4. Que las condiciones restantes se mantengan inalteradas.

10.5.5. La última actualización se entenderá, entre otras cosas, como que el bien esté en línea de producción al momento de la entrega, o como la última versión del fabricante, cuando el objeto admita actualizaciones de esa naturaleza y ésta haya sido conocida en el mercado al menos un mes antes de la entrega de la orden de inicio. Para estos efectos, el oferente deberá respaldar el ofrecimiento con certificación emitida directamente por el fabricante.

10.5.6. La mejora deberá informarse por escrito, explicando en detalle en qué consiste el cambio, de ser necesario a partir de literatura técnica y cualesquiera otros elementos que resulten pertinentes.

10.5.7. Bajo ninguna circunstancia, los cambios en los bienes o servicios podrán demeritar las garantías y condiciones de los bienes inicialmente ofrecidas, las cuales se consideran un mínimo que no podrá ser rebajado ante modificaciones de esta naturaleza.

11. OBLIGACIONES DEL ADJUDICADO

11.1. Se requiere que la persona jurídica adjudicada realice en coordinación con el Proceso Informática de la Municipalidad de Escazú la instalación o desinstalación del software ofertado por parte de personal técnico de la persona jurídica adjudicada.

11.2. La persona jurídica adjudicada debe realizar la instalación en el sitio de la licencia, esto con personal técnico de la persona jurídica adjudicada especializado y certificado por la solución y para su debida implementación.

11.3. De presentarse diferencias con respecto a los bienes ofertados, la persona jurídica adjudicada deberá proceder, bajo su costo, a sustituirlo sin costo adicional para la Municipalidad.

11.4. El recibido conforme se le dará a la persona jurídica adjudicada cuando el Proceso Informática de la Municipalidad de Escazú brinde su aprobación. Para dar la aprobación, los bienes deberán estar completamente instalados según especificaciones descritas en este cartel y que se ejecute el mismo para verificar que la licencia funciona adecuadamente.

11.5. La Municipalidad se reserva el derecho de que sus técnicos y asesores técnicos comprueben, durante las pruebas la calidad de las licencias que se adjudicaron.

11.6. El adjudicado debe cumplir con los siguientes **requisitos mínimos:**

11.6.1. El proveedor adjudicado debe indicar el procedimiento para reportes y atención de fallas, así como para el control de una respuesta efectiva. El tiempo de respuesta, dentro del horario contratado, para atender directamente la falla, ***no debe ser mayor ocho (8) horas***. Este horario ofrecido debe incluir al menos las horas de las 7:30 a.m. a las 4:00 p.m., de lunes a viernes. Debe indicarse el costo de atención de fallas fuera del horario ofrecido, incluyendo noches, sábados y domingos.

11.6.2. Presentar lista de referencia de empresas o instituciones que hayan adquirido licencias similares, en un plazo no mayor de tres (3) años atrás, indicando licencias vendidos, empresa, persona contacto y número de teléfono.

11.6.3. La oferta debe estar escrita en español y acompañarse de literatura técnica descriptiva, completa y detallada del software ofrecido para cada rubro por separado, en donde se exprese en forma clara y amplia cada una de sus características técnicas y físicas, en idiomas español o inglés.

11.6.4. La persona jurídica adjudicada debe cumplir con los siguientes requisitos ***mínimos***:

11.6.4.1. Garantizar la existencia y suministros de bienes. La institución aplicará las sanciones contra el proveedor que no cumpla con esta condición, tal como lo establece la legislación vigente.

11.6.4.2. La oferta debe estar escrita en español y de ser necesario acompañarse de literatura técnica descriptiva, completa y detallada del material, de todos los componentes ofrecidos para cada rubro por separado, en donde se exprese en forma clara y amplia cada una de sus características técnicas y físicas, en idioma español o inglés.

11.6.4.3. ***Consolidación de la Empresa***: el adjudicado debe tener un mínimo de dos años (2) años de ser distribuidor de rubros como los ofertados, en el mercado costarricense

A efectos de probar tal consolidación, el adjudicado deberá aportar una lista, bajo fe de juramento, de las ventas hechas del tipo de rubro mencionado, en el mercado costarricense, durante los últimos dos años, con indicación del nombre y teléfono del comprador. La Municipalidad se reserva el derecho de verificar los datos consignados en la lista y hasta solicitar documentos en donde se demuestre que ha distribuido equipos y/o software en el mercado costarricense.

11.6.4.4. ***Consolidación de la Marca***: el adjudicado debe demostrar la venta, durante al menos dos (2) años, en el mercado costarricense, de rubros similares a los solicitados, de modelos o versiones anteriores o iguales, y de la misma marca ofertada (no importa el distribuidor local que los haya vendido).

11.6.5. La persona jurídica será responsable de la sustitución y reemplazo de los problemas de los bienes entregados, cuando los mismos sean consecuencia de hechos imputables, excepto en los casos fuerza mayor o caso fortuito.

En aquellos casos, donde los daños originados de uso inadecuado, perdida, robo o extravío son generados por los funcionarios municipales asignados, este aspecto que deberá acreditarse debidamente por escrito con el respaldo técnico y pruebas suficientes de ser necesario, detallando costo de la sustitución y el costo del reemplazo del material.

Al respecto, la Municipalidad de Escazú tendrá un plazo de ocho (8) días hábiles para resolver la aceptación o rechazo de la petición aportada. Sin embargo, la persona jurídica deberá en toda instancia atender el reemplazo del material de forma inmediata.

12. EXPERIENCIA DEL OFERENTE

12.1. Como requisito de admisibilidad los oferentes deberán demostrar que cuentan con experiencia positiva mínima de tres (3) años en la prestación en el desarrollo de proyectos de seguridad similares al solicitado en este pliego cartelario, demostrado con la aportación la tabla de referencia. Además, aportar listado de proyectos, ubicados a nivel nacional y / o internacionales, a los cuales les ha brindado el servicio según la siguiente tabla.

Persona Contacto	Empresa	Descripción Proyecto	Persona Encargada de Implementar el Proyecto	Fecha Inicio (dd/mm/aaaa)	Fecha Final (dd/mm/aaaa)	Teléfono

Únicamente se tomará en cuenta la experiencia indicada en proyectos iniciados y finalizados entre los años dos mil doce (2012) al año dos mil quince (2015)

La tabla de referencia será verificada por Proceso Informática. La oferta que no cumpla con la experiencia mínima solicitada será excluida automáticamente de este concurso y no será tomada en cuenta para efectos de calificación.

12.2. La empresa deberá estar certificada al menos a un nivel Gold o equivalente por la marca de productos ofertados.

12.3. La empresa deberá aportar lista de clientes con la identificación de los mismos y que en la actualidad utilizan el producto (nombre de la empresa, teléfono, correo electrónico y contacto) de encontrarse falsedad en la información dicha oferta será excluida del proceso.

12.4. Requerimientos de personal técnico y profesional para el desarrollo de la contratación.

12.5. La empresa oferente deberá asignar un encargado de la instalación, el cual será el punto de contacto con los profesionales asignados por la Municipalidad, a saber, el inspector y el responsable del proyecto por parte de la Municipalidad o Director del proyecto, por lo que deberá tener potestad y autoridad necesaria de tomar decisiones relativas al alcance del trabajo y cualquier modificación o cambio que sea requerido, y estar dedicado a tiempo completo al proyecto.

12.6. La empresa deberá aportar los siguientes profesionales:

Cantidad	Personal Técnico	Copia Certificados	Experiencia
1	Ingeniería en Electrónica o Sistemas Informáticos. “Obligatorio presentar copia título que lo acredite como Ingeniero”.	Certificado como experto en seguridad red, que posea conocimientos y habilidades de cómo configurar y mantener un Sistema de Gestión Unificada de Amenazas, ITIL o COBIT	Dos (2) Años

13. OBLIGACIONES LABORALES

13.1. La persona jurídica adjudicada tiene el deber y la obligación ineludible de cumplir con sus obligaciones laborales y de seguridad social para con sus trabajadores.

13.2. En caso de incumplimiento comprobado en el régimen de seguridad social, ello se tendrá como incumplimiento contractual que facultará a la Municipalidad de Escazú para dar por resuelto el vínculo contractual con las eventuales ejecuciones de las garantías de cumplimiento y demás sanciones aplicables.

13.3. De previo a la tramitación de cada pago que sobrevenga, producto de esta prestación, el Proceso Informática de la Municipalidad de Escazú deberá exigir la presentación de la documentación que demuestre la adecuada cobertura de estas obligaciones por parte de la persona jurídica adjudicada.

13.4. La contratación de estos servicios no originará relación de empleo público entre la Administración y la persona jurídica adjudicada; por lo que los costos originados por concepto de cargas sociales y seguros correrán por cuenta de la persona jurídica adjudicada.

13.5. El personal contratado deberá cumplir con el ordenamiento jurídico vigente en materia de Salud Ocupacional.

13.6. La persona jurídica adjudicada antes del inicio del proyecto suscribirá de su propio peculio, y bajo su responsabilidad, una póliza de riesgos de trabajo y póliza de responsabilidad civil con el Instituto Nacional de Seguros y la póliza deberá cubrir por el monto total del contrato, y contar con una vigencia igual a la duración del proyecto.

13.7. Es entendido que la persona jurídica adjudicada libera a la Municipalidad de Escazú, de toda responsabilidad patronal, ya que se constituirá un contrato no afecto a relación laboral. Lo anterior, será verificado por el Proceso Cultura.

14. METODOLOGÍA DE CALIFICACIÓN

La asignación de puntaje máximo por aspecto a evaluar es el siguiente.

14.1. Precio 80%

Se evaluará tomando en cuenta el factor precio en un 80%, todo en ecuaciones proporcionalmente decreciente al mejor factor ofrecido.

$$FP = \frac{P1}{P2} \times 80\%$$

Donde:

P1 será la oferta de menor precio.

P2 será la oferta a calificar.

14.2. Experiencia Positiva 20%

Se evaluará tomando en cuenta el factor experiencia positiva en la prestación del servicio de venta o arrendamiento de equipo de cómputo en condiciones similares en un 20% sea en Costa Rica como en otros países de la región Centroamericana, según tabla adjunta y medida en meses cumplidos. Para demostrar la experiencia profesional, se deberá aportar los requisitos indicados en el punto N° 12 del Capítulo Segundo del pliego de condiciones.

Experiencia	20,00%
De 36 meses a 48 meses	10,00%
De 49 meses a 60 meses	15,00%
Más de 61	20,00%

Se tomarán en cuenta únicamente los proyectos que cuenten con una prestación en el desarrollo de proyectos de seguridad en los últimos cinco (5) años (2011, 2012, 2013, 2014 y 2015). Únicamente se tomará en cuenta la experiencia indicada en proyectos iniciados y finalizados durante el periodo solicitado.

No se aceptará la experiencia de empresas subcontratadas.

15. MEDIDAS DE VERIFICACIÓN Y CONTROL

15.1. La Municipalidad de Escazú dispone de una persona encargada en el Proceso de Informática, o bien la persona que esté como titular en ese momento, quién realizará la comprobación y verificación para que la contratación se cumpla con las especificaciones técnicas indicadas en el presente cartel.

15.2. El Proceso de Informática de la Municipalidad de Escazú ejercerá la supervisión del avance del proyecto, en momentos seleccionados al azar, si se comprobara cualquier tipo de anomalía, la Administración se reserva el derecho de rescindir, según lo indicado en el Artículo N° 204 del Reglamento a la Ley de Contratación Administrativa.

15.3. Verificar que los inicios del servicio coincidan con la orden de inicio dictada.

15.4. Se mantendrá una comunicación fluida con la persona adjudicada con el fin de fiscalizar que esta cumpla con el pliego de condiciones.

15.5. Las condiciones específicas del objeto contractual son responsabilidad directa del área solicitante y técnica, no del Proceso Proveeduría. Todo a la luz del Principio de Eficiencia y Eficacia que rige la materia de Contratación Administrativa

15.6. En caso de duda la administración podrá realizar la verificación de los documentos, constancias, certificaciones, y otros aportados por los oferentes que considere necesario.

16. FORMA DE PAGO

16.1. Se pagará contra entrega a satisfacción de la Municipalidad y para ello debe presentar las facturas originales timbradas en el Proceso de Informática.

16.2. La Municipalidad tendrá un máximo de treinta (30) días naturales para pagar, previa presentación de la factura y previa verificación del cumplimiento a satisfacción de conformidad con lo indicado en este cartel.

16.3. Toda transacción debe respaldarse con facturas o comprobantes que reúnan los requisitos establecidos por la Dirección General de la Tributación Directa. Las empresas a las que se les haya dispensado del trámite de timbraje, deberán hacer referencia en las facturas o comprobantes que presenten ante la Municipalidad de Escazú, del número de resolución mediante la cual se les eximió de ese trámite. La Municipalidad de Escazú no se responsabiliza por los atrasos que puedan darse en la fase de ejecución, con motivo del incumplimiento de este aspecto.

16.4. Los pagos se realizarán en colones costarricenses y sujeto a la cantidad de bienes.

16.5. En caso de cotizaciones en dólares de los Estados Unidos de América, se utilizará el tipo de cambio de venta de referencia que reporte el Banco Central de Costa Rica para el día en que se emite el pago.

16.6. Para estos efectos el oferente tramitará la factura original timbrada respectiva ante el Proceso Informática de la Municipalidad de Escazú.

16.7. Se adjunta tabla de bienes requeridos, que funcionará como base general, esto lógicamente estará muy ligado a los bienes requeridos.

TABLA DE BIENES REQUERIDOS

"Contratación de Equipos de Seguridad Informática Perimetral"

Ítem	Cantidad	Unidad de Pago	Descripción	Precio Unitario en Números	Monto Total Propuesto
1	1	Unidad	Contratación de Equipo de Seguridad Informática Perimetral para Palacio Municipal		
2	1	Unidad	Contratación de Equipo de Seguridad Informática Perimetral para Edificio Pedro Arias		
3	1	Unidad	Appliance para Consolidación de Logs y Administración de Reportes		

16.8. El sistema de pago se verá interrumpido por la suspensión del contrato, la cual será indicada por el área técnica.

16.9. Los oferentes deberán indicar el número de Cuenta Corriente en cl Banco Nacional de Costa Rica o en su defecto el número de Cuenta Cliente SINPE, para efectos de trámite de pago por ese medio de ser posible por la Municipalidad de Escazú.

16.10. Se advierte que de no tramitarse el pago antes de concluir actividades en diciembre, este pasará a trámite de liquidación y quedará como compromiso pendiente para pagar en el año dos mil diecisiete (2017). Por lo que se suspenderá el pago de actividades hasta que la Contraloría General de la República otorgue la aprobación al presupuesto respectivo.

17. CLAUSULA PENAL

17.1. ***Por incumplimiento en la fecha de inicio de labores***

En caso de no cumplir con la fecha de inicio fijada por la Municipalidad de Escazú, ésta cobrará una multa por cada día de retraso equivalente al 2% de la cuantía resultante de sumar los montos correspondientes a los servicios indicados en el pliego de condiciones, los que serían multiplicados por los precios unitarios que fueron ofertados por la persona jurídica adjudicada, para los servicios contratados.

Como se indica, dicho ejercicio será realizado por cada día natural de atraso, hasta alcanzar un máximo del 25% de la facturación mensual estimada, alcanzada dicha cuantía se tendrá por incumplido el contrato sin responsabilidad para la Municipalidad de Escazú.

17.2. ***Por incumplimiento de las características de los servicios bajo contrato***

De producirse un incumplimiento en las características de los servicios suministrados a la Municipalidad de Escazú, se cobrará una multa del 5% sobre valor pactado para dichos servicios, que se debió haber prestado, y la persona jurídica adjudicada deberá efectuar la reposición en un término de 24 horas hábiles. En caso de incumplimiento de dicho plazo se aplicará la multa por incumplimiento en plazos de entrega, establecida en el punto anterior. La suma que corresponda por concepto de la aplicación de esta cláusula, será rebajada del pago que se le haga al contratista y será aplicada únicamente a los bienes que incumplan las especificaciones pactadas.

17.3. La Municipalidad de Escazú podrá solicitar la resolución del contrato de conformidad con lo establecido en el Artículo N° 204 del Reglamento a la Ley de Contratación Administrativa.

17.4. Las multas se cobrarán deduciéndolas de las facturas que se presenten al cobro posterior a haber acaecido el hecho, siguiendo el procedimiento legal respectivo. Se podrá retener un 10% de los pagos hasta el pago siguiente para de esa forma cobrar las multas.

18. REVISIÓN DE PRECIOS

18.1. Según lo establecido en el Artículo N° 18 de la Ley de Contratación Administrativa y en el Artículo N° 31 del Reglamento a la Ley de Contratación Administrativa las partes tendrán derecho al ajuste o revisión de precios siempre que se acredite la variación de los respectivos costos conforme las reglas existentes.

18.2. En caso de reajuste de precios se requiere que los oferentes indiquen en renglones separados: los costos directos, los costos indirectos, las utilidades y los imprevistos. Se recurrirá a la fórmula indicada en el Reglamento para el Reajuste de Precios en los Contratos de Obra Públicas de Construcción y Mantenimiento, publicada en el Diario Oficial La Gaceta N° 94 del 17 de mayo de dos mil seis, Transitorio N° 11. El oferente deberá indicar en su oferta cual utilizará.

18.3. En todo caso, el reconocimiento que se llegue a otorgar se contará a partir del momento en que la persona jurídica adjudicada formule la solicitud y aporte la documentación probatoria a satisfacción de la Municipalidad de Escazú.

18.4. En el caso de las ofertas cuyo precio se cotice en dólares no procede el reajuste de precios por medio de la metodología definida en el Reglamento para el Reajuste de Precios en los Contratos de Obra Públicas de Construcción y Mantenimiento, sino que para solicitar el reconocimiento que surja del incremento en los costos del servicio no cubiertos por las políticas de valuación del colón frente al dólar americano, la persona jurídica adjudicada deberá presentar reclamos administrativos posteriores a los pagos correspondientes, en los cuales tendrá la obligación de demostrar el desequilibrio económico correspondiente a cada mes reclamado.

18.5. El pago se efectuará después de la aprobación ante la Contraloría General de la Repúblicas del presupuesto extraordinario que se realice posterior a la solicitud de la revisión de precios.

Atentamente

Alberto Arias Víquez
Informática