GOBIERNO DE LA
REPÚBLICA DOMINICANA
CULTURA

ADQUISICIÓN DE SISTEMA DE SEGURIDAD Y PROTECCIÓN CONTRA AMENAZAS AVANZADAS DE PERÍMETRO Y ENDPOINTS CON CAPACIDAD PARA 300 USUARIOS Y SUS EQUIPOS SERVIDORES PARA SER INSTALADOS EN EL DATACENTER DE ESTE MINISTERIO DE CULTUIRA.

COMPARACION DE PRECIO

CULTURA-CCC-CP-2021-0023

Santo Domingo, Distrito Nacional
República Dominicana
Septiembre, 2021

TABLA DE CONTENIDO

COMPARACIÓN DE PRECIOS DE BIENES Y SERVICIOS……..3
1.1 Objeto……3
1.2 Presentación de Ofertas……3
1.3 Condiciones de Pago……3
1.4 Moneda de la Oferta……3
1.5 Documentos a Presentar……3
1.6 Forma de Presentación de los Documentos contenidos en el Sobre……4
1.7 Cronograma de la Comparación de Precios de Bienes y Servicios……5
1.8 Condiciones Generales del Contrato……6
1.8.1 Garantía de Fiel Cumplimiento del Contrato……6
1.8.2 Devolución de las Garantías……6
1.8.3 Efectos del Incumplimiento……7
1.8.4 Penalidades……7
1.8.5 Vigencia del Contrato……7
1.9 De los Oferentes/Proponentes Hábiles e Inhábiles……7
1.9.1 Prohibición de contratar……7
1.10 Enmiendas……9
1.11 Otros Requisitos……9
1.12 Errores No Subsanables del Proceso……9
2. ESPECIFICACIONES TÉCNICAS……10
2.1 Criterio de Evaluación……14

2.2 Evaluación Técnica……14

2.3 Evaluación Económica…… ……15

1. DATOS DE LA COMPARACIÓN DE PRECIOS DE BIENES Y SERVICIOS

1.1 Objeto

Constituye el objeto de la presente convocatoria la contratación del servicio de "adquisición de sistema de seguridad y protección contra amenazas avanzadas de perímetro y endpoints con capacidad para 300 usuarios y sus equipos servidores para ser instalados en el datacenter de este Ministerio de Cultuira", de acuerdo con las condiciones fijadas en las presentes Especificaciones Técnicas. La adjudicación se hará a favor del Oferente que presente la mejor propuesta y que cumpla con las especificaciones técnicas requeridas, sea calificado como la Oferta que más convenga a la satisfacción del interés general y el cumplimiento de los fines y cometidos de la administración conforme a especificaciones y precio.

1.2 Presentación de Ofertas

La presentación de Propuestas se efectuará en acto público, ante el Comité de Compras y Contrataciones y el Notario Público en la Sala de Conferencias del segundo nivel, ubicada en la Avenida George Washington esquina Presidente Vicini Burgos, del día indicado en el Cronograma del proceso y sólo podrá postergarse por causas de Fuerza Mayor o Casos Fortuitos definidos en el presente Pliego de Condiciones Específicas. Una vez pasada la hora establecida para la recepción de los Sobres de los Oferentes/Proponentes, no se aceptará la presentación de nuevas propuestas, aunque el acto de apertura no se inicie a la hora señalada.

1.3 Condiciones de Pago

El término del contrato es por un (1) año y la condición de pago será contra presentación de la factura según el servicio requerido.

1.4 Moneda de la Oferta

El precio en la Oferta deberá estar expresado en moneda nacional, (Pesos Dominicanos, RD$).

1.5 Documentos a Presentar

Sobre A

1. Formulario de Presentación de la Oferta (Formulario SNCC.F.034).
2. Formulario de Información sobre el Oferente (Formulario SNCC.F.042).
3. Registro de Proveedores del Estado (RPE).
4. Copia certificada del Registro Mercantil vigente en caso de ser persona jurídica.
5. Documentos constitutivos de la empresa, incluyendo la última Asamblea realizada.
6. El objeto social de la empresa debe ser compatible con la venta y/o contratación de servicios, según el rubro inscrito en el catálogo dispuesto por la DGCP.

7. Acta de Delegación de Poderes, si procede. (Para los casos que se delegue a alguien que no tenga facultades de gerencia o administración la representación de la sociedad comercial en el proceso).

8. Declaración Jurada que manifieste: (1) que no se encuentra dentro de las prohibiciones establecidas en el Artículo 14 de la Ley 340-06, ni de las prohibiciones señaladas en el presente pliego de condiciones y, donde se manifieste: (2) si tiene o no juicio con el Estado Dominicano o sus entidades del Gobierno Central, de las Instituciones Descentralizadas y Autónomas no financieras y de las Instituciones Públicas de la Seguridad Social, (3) si está sometida a un proceso de quiebra o bancarrota, en estado de cesación de pagos o reestructuración, (4) si está o no bajo secuestro administración judicial; (5) si está o no al día en el pago de las obligaciones fiscales y de seguridad social; y (6) Que sus socios administradores, representante legal, gerentes y agentes autorizados indicados no tienen antecedentes penales.

9. Carta confirmando aceptación de condiciones de pago, tiempo y lugar donde realizará la prestación del servicio.

10. Copia de la Cédula de Identidad y Electoral del representante quien firmará el contrato en caso de resultar adjudicatario, con indicación de la posición ocupada en la empresa participante.

11. Copia de certificación de MIPYME, si aplica.

12. Oferta Técnica (De acuerdo a las especificaciones técnicas requeridas).

13. Certificación actualizada emitida por la Dirección General de Impuestos Internos, en la cual se haga constar que la empresa se encuentra al día en el pago de impuestos.

14. Certificación emitida por la Tesorería de la Seguridad Social (TSS). en la que se haga constar que se encuentra al día en el cumplimiento de las obligaciones sociales.

15. Referencias bancadas que avalen una línea de crédito disponible para la ejecución del presente proyecto.

16. Referencias comerciales que validen el buen servicio en proyectos similares al requerido en este pliego de condiciones.

17. Estados Financieros, del último ejercicio fiscal contable, debidamente auditado.

Sobre B

18. Formulario de Presentación de la Oferta Económica (SNCC.F.033). Conteniendo la información siguiente:
    - ITBIS transparentado. (El ITBIS debe reflejarse en cada precio unitario y debe ser totalizado al final de la cotización).

19. Garantía de Seriedad de la Oferta Original. Correspondiente a una Garantía Bancaria o Póliza de Seguros a disposición del Ministerio de Cultura, emitida por una entidad bancaria o

aseguradora de reconocida solvencia en el país, por un valor de 1% del monto de la Oferta Económica en moneda local (RD$), con fecha de vigencia mínima aceptada hasta 60 días a partir de la fecha de la presentación de su oferta económica. De no presentar dicha garantía o si resultase insuficiente, su Oferta quedará descalificada sin más trámite.

Nota Importante:

- El Ministerio de Cultura no recibirá sobres que no estén debidamente cerrados e identificados.
- Las Ofertas que se presenten en Sobres Abiertos no serán recibidas.
- En el caso de entregar su oferta incompleta, es decir un sobre sí, faltando el otro, será descalificada sin más trámite.
- Las Ofertas que en el Sobre A (Propuesta Técnica), presenten documentación que son parte del Sobre B (Propuesta Económica) o viceversa, se auto-descalifican sin más trámite.
- No podrán participar al mismo tiempo empresas controlantes, vinculadas o subsidiarias o que estén relacionadas por formas similares o equivalentes.

1.6 Forma de Presentación de los Documentos Contenidos en el Sobre.

Los documentos contenidos en el sobre deberán ser presentados en un (01) original debidamente marcado como “ORIGINAL "en la primera página del ejemplar, junto con dos (2) fotocopias simples de los mismos, debidamente marcada, en su primera página, como “COPIA".

Los documentos deben estar organizados según el orden planteado anteriormente y divididos por separadores (pestañas). Al igual que, debidamente encuadernados.

El original y las copias deberán firmarse en todas las páginas por el Representante Legal, debidamente foliadas v deberán llevar el sello social de la compañía.

Las Ofertas deberán contener en su cubierta la siguiente identificación:

Nombre del OFERENTE/PROPONENTE
(Sello Social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
MINISTERIO DE CULTURA
PRESENTACIÓN DE OFERTA TÉCNICA Y ECONÓMICA
Atención:
REFERENCIA: CULTURA-CCC-CP-2021-0023

El Oferente que adquiera la ficha técnica a través de la página Web de la Institución, www.cultura.gob.do o del portal administrado por el Órgano Rector, www.comprasdominicana.gov.do. deberá enviar un correo electrónico notificando al Departamento de Compras del Ministerio de Cultura, sobre la adquisición del mismo, a los fines de que la Entidad Contratante tome conocimiento de su

interés en participar. Para fines de consultar, canalizarlas a través del correo de correspondiente al concurso.

Datos de contacto:

Atención:
Referencia: CULTURA-CCC-CP-2021-0004

Dirección: Avenida George Washington esquina Presidente Vicini Burgos.
Teléfonos: 809-221-4141
Correo: compras@minc.gob.do

1.7 Cronograma de la Comparación de Precios de Bienes y Servicios

Detalle	Fecha y hora
Fecha de publicación del aviso de convocatoria	28/9/2021 11:00
Presentación de aclaraciones	1/10/2021 16:00
Reunión aclaratoria	
Plazo máximo para expedir Emisión de Circulares, Enmiendas y/o Adendas	5/10/2021 13:30
Presentación de Credenciales/Ofertas técnicas y Ofertas Económicas	7/10/2021 11:00
Apertura de Credenciales/Ofertas técnicas	8/10/2021 10:00
Verificación, Validación y Evaluación de Credenciales/Ofertas técnicas	8/10/2021 10:05
Informe Preliminar de Evaluación de Credenciales/Ofertas técnicas	8/10/2021 10:10
Notificación de Errores u Omisiones de Naturaleza Subsanable	8/10/2021 15:30
Ponderación y Evaluación de Subsanaciones	11/10/2021 11:00
Notificación de Oferentes Habilitados para presentación de Oferta Económica	11/10/2021 13:00
Apertura Oferta Económica	12/10/2021 10:00
Evaluación de Ofertas Económicas	12/10/2021 11:00
Acto de Adjudicación	12/10/2021 16:00
Notificación de Adjudicación	12/10/2021 16:30
Constitución de Garantía de Fiel Cumplimiento	18/10/2021 16:30
Suscripción del Contrato	28/10/2021 16:30
Publicación del Contrato	28/10/2021 17:30

Nota.: El formato de este cronograma ha sido tomado directamente del proceso en el Portal Transaccional.

1.8 Condiciones Generales del Contrato

1.8.1 Garantía de Fiel Cumplimiento de Contrato

Los Adjudicatarios cuyos Contratos excedan el equivalente en Pesos Dominicanos de diez mil Dólares Americanos con 00/100 (US$10,000.00) están obligados a constituir una Fianza emitida por una aseguradora de reconocida solvencia en la República Dominicana o Garantía Sanearía (con la condición de ser está incondicional, irrevocables y renovables), en el plazo de cinco (5) días hábiles, contados a partir de la Notificación de la Adjudicación, por el importe del cuatro por ciento (4%) del monto total del Contrato a intervenir, a favor del Ministerio de Cultura de la República Dominicana. La no comparecencia del Oferente Adjudicatario a constituir la Garantía de Fiel Cumplimiento de Contrato, se entenderá que renuncia a la Adjudicación y se procederá a la ejecución de la Garantía de Seriedad de la Oferta y a las demás acciones que legalmente correspondan. En el caso de que el adjudicatario sea una Micro, Pequeña y Mediana empresa (MIPYME) el importe de la garantía será de un UNO POR CIENTO (1%). La Garantía de Fiel Cumplimiento de Contrato debe ser emitida por una entidad bancaria de reconocida solvencia en la República Dominicana.

Cuando hubiese negativa a constituir la Garantía de Fiel Cumplimiento de Contrato, el MINC, como órgano de ejecución del contrato, notificará la adjudicación de los renglones correspondientes al Oferente que hubiera obtenido la siguiente posición en el proceso de adjudicación, conforme al informe Final del proceso. El nuevo Oferente Adjudicatario depositará la Garantía y suscribirá el Contrato de acuerdo al plazo que le será otorgado por la MINC, mediante comunicación formal. –

1.8.1.1 Vigencia de Garantía Fiel Cumplimiento de Contrato

El Llamado a Comparación de Precios se hace sobre la base de los Servicios de impresión en un periodo de un (1) año, contados a partir de la firma del contrato.

La vigencia de la garantía será de doce (12) meses, contados a partir de la constitución de la misma hasta el fiel cumplimiento del contrato según la fecha de suscripción prevista en el cronograma. En caso de que sea prorrogado el contrato por causas atendibles, el proveedor deberá extender la vigencia de dicha garantía por el término extendido.

1.8.2 Devolución de las Garantías

a) Garantía de la Seriedad de la Oferta: Tanto al Adjudicatario como a los demás oferentes participantes una vez integrada la garantía de fiel cumplimiento de contrato.

b) Garantía de Fiel Cumplimiento del Contrato y Garantía de Adjudicaciones Posteriores:

   Después de aprobada la liquidación del Contrato, si no resultaren responsabilidades que conlleven la ejecución de la Garantía y transcurrido el plazo de la misma, se ordenará su devolución.

1.8.3 Efectos del Incumplimiento

El incumplimiento del contrato y/o orden de compra o servicios por parte del adjudicatario determinará su finalización y supondrá para el mismo la ejecución de la Garantía de Fiel Cumplimiento del Contrato, procediéndose a contratar el adjudicatario que haya quedado en segundo lugar.

En los casos en que el incumplimiento del Proveedor constituya falta de calidad de los bienes entregados o causare un daño o perjuicio a la institución, o a terceros, el Ministerio de Cultura de la República Dominicana podrá solicitar a la Dirección General de Contrataciones Públicas, en su calidad de Órgano Rector del Sistema su inhabilitación temporal o definitiva, dependiendo de la gravedad de la falta.

1.8.4 Penalidades

En caso de demoras en el cumplimiento del contrato: a) A partir de dos (2) días hábiles de interrupción del servicio, y si el proveedor no notificó por escrito, indicando las razones de la interrupción, el MINC descontará un 0.5% del monto de la mensualidad por cada día en que se mantenga la interrupción del servicio, b) A partir de cinco (5) días hábiles se descontará el 1% del monto de la mensualidad por cada día que se mantenga la interrupción del servicio.

En los casos en que el MINC compruebe, al momento de la ejecución del servicio, que no cumple con las especificaciones técnicas requeridas, no será recibido y la penalización será acorde con lo establecido en el párrafo anterior con relación a los días de interrupción del servicio.

1.8.5 Vigencia del Contrato

La vigencia del Contrato será por doce (12) meses a partir de la firma y hasta su fiel cumplimiento, de conformidad con el Cronograma de Trabajo, el cual formará parte integral y vinculante del mismo.

1.9 De los Oferentes/Proponentes Hábiles e Inhábiles

Toda persona natural o jurídica, nacional o extranjera que haya adquirido los Términos de Referencia (TDRs), tendrá derecho a participar en la presente comparación, siempre y cuando reúna las condiciones exigidas y no se encuentre afectada por el régimen de prohibiciones establecido en los presentes Términos de Referencia.

1.9.1 Prohibición de contratar

No podrán participar como oferentes/ proponentes, en forma directa o indirecta, las personas físicas o sociedades comerciales que se relacionan a continuación:

1) El Presidente y Vicepresidente de la República; Los Secretarios y Subsecretarios de Estado; los Senadores y Diputados del Congreso de la República; los Magistrados de la Suprema Corte de Justicia, de los demás tribunales del orden judicial, de la Cámara de Cuentas y de la Junta Central Electoral; los Síndicos y Regidores de los Ayuntamientos de los Municipios y del Distrito Nacional; el

Contralor General de la República y el Subcontralor; el Director de presupuesto y Subdirector; el Director Nacional de Planificación y el Subdirector; el Procurador General de la República y los demás miembros del Ministerio Público; el Tesorero Nacional y el Subtesorero y demás funcionarios de primer y segundo nivel de jerarquía de las instituciones incluida bajo el ámbito de aplicación de la Ley 340-06;

2) Los jefes y subjefes de Estado Mayor de las Fuerzas Armadas, así como el jefe y subjefe de a Policía Nacional;

3) Los funcionarios públicos con injerencia o poder de decisión en cualquier etapa del procedimiento de contratación administrativa;

4) Todo el personal de la entidad contante;

5) Los parientes por consanguinidad hasta el tercer grado o por afinidad hasta el segundo grado, inclusive, de los funcionarios relacionados con la contratación cubiertos por la prohibición, así como los cónyuges, las parejas en unión libre, las personas vinculadas con análoga relación de convivencia afectiva o con las qu hayan procreado hijos, y descendientes de estas personas;

6) Las personas jurídicas en las cuales las personas naturales a las que se refieren los Numerales 1 al 4 tengan una participación superior al diez por ciento (10%) del capital social, dentro de los seis meses anteriores a la fecha de la convocatoria;

7) Las personas físicas o jurídicas que hayan intervenido como asesoras en cualquier etapa del procedimiento de contratación o hayan participado en la elaboración de las especificaciones técnicas o los diseños respectivos, salvo en el caso de los contratos de supervisión;

8) Las personas físicas o jurídicas que hayan sido condenadas mediante sentencia que haya adquirido la autoridad de la cosa irrevocablemente juzgada por delitos de falsedad o contra la propiedad, o por delitos de cohecho, malversación de fondos públicos, tráfico de influencia, prevaricación, revelación de secretos, uso de información privilegiada o delitos contra las finanzas públicas, hasta que haya transcurrido un lapso igual al doble de la condena. Si la condena fuera por delito contra la administración pública, la prohibición para contratar con el Estado será perpetua;

9) Las empresas cuyos directivos hayan sido condenados por delitos contra la administración pública, delitos contra la fe pública o delitos comprendidos en las convenciones internacionales de las que el país sea signatario;

10) Las personas físicas o jurídicas que se encontraren inhabilitadas en virtud de cualquier ordenamiento jurídico;

11) Las personas que suministrasen informaciones falsas o que participen en actividades ilegales o fraudulentas relacionadas con la contratación;

12) Las personas naturales o jurídicas que se encue3ntren sancionadas administrativamente con inhabilitación temporal o permanente para contratar con entidades del sector público, de acuerdo a lo dispuesto por la presente ley y sus reglamentos;

13) Las personas naturales o jurídicas que no estén al día en el cumplimiento de sus obligaciones tributarias o de la seguridad social, de acuerdo con lo que establezcan las normativas vigentes;

PÁRRAFO 1: Para los funcionarios contemplados en los Numerales 1 y 2. la prohibición se extenderá hasta seis meses después de la salida del cargo,

PÁRRAFO II; Para las personas incluidas en los Numerales 5 y 6 relacionadas con el personal referido en el Numeral 3. la prohibición será de aplicación en el ámbito de la institución en que estos últimos prestan servicios.

En adición a las disposiciones del artículo 14 de la Ley 340-06 con sus modificaciones NO podrán ser Oferentes ni contratar con el Estado Dominicano, los Oferentes que hayan sido inhabilitados temporal o permanentemente por la Dirección General de Contrataciones Públicas en su calidad de Órgano Rector. Tampoco podrán contratar con el Estado dominicano los proveedores que no hayan actualizado sus datos en el Registro de Proveedores del Estado.

1.10 Enmiendas

De considerarlo necesario, por iniciativa propia o como consecuencia de una consulta, el Comité de Compras y Contrataciones podrá modificar, mediante enmiendas, las Especificaciones Técnicas, formularios, otras Enmiendas anexos. Las enmiendas se harán de conocimiento de todos los Oferentes/Proponentes y se publicarán en el portal institucional y en el administrado por el Órgano Rector.

Tanto las enmiendas como las circulares emitidas por el Comité de Compras y Contrataciones pasarán a constituir parte integral las Especificaciones Técnicas y en consecuencia, serán de cumplimiento obligatorio para todos los Oferentes/Proponentes.

1.11 Otros Requisitos

- Las Ofertas Económicas deberán ser presentadas única y exclusivamente en el formulario designado al efecto por el Ministerio de Cultura, siendo inválida toda oferta bajo otra presentación.
- Los proveedores internacionales que deseen participar deben hacerlo a través de un representante local.
- Tiempo de ejecución: Un año (1).

1.12 Errores No Subsanables del proceso

Los errores NO subsanables en este procedimiento de contratación son:

- La omisión de la Garantía de la Seriedad de la Oferta en original, o cuando la misma fuera insuficiente (en cuanto a tiempo, monto y vigencia, así como una constitución de póliza con objeto erróneo).
- Presentación de la Oferta Económica en un formato diferente al formulario establecido suministrado por la DGCP.
- Presentar productos o servicios diferentes a los solicitados, o excluir algún ítem necesario para la realización de la propuesta.

Nota: Los documentos o informaciones subsanables deberán ser entregados en papel timbrado de la empresa con firma y sello del representante legal, en la fecha indicada en el cronograma de actividades de la presente Comparación de Precios.

2. ESPECIFICACIONES TÉCNICAS

A continuación, se presenta la descripción mínima requerida de las especificaciones técnicas.

No. De Partida	**Cantidad**	***Descripción***	**Especificaciones Técnicas**
		Sistemas de Seguridad Lógica	***Sistemas de Seguridad Lógica integrada Ministerio de Cultura***
A.0100		***Condiciones Generales a ser ofertadas y cumplidas para todas las soluciones ofertadas en este lote:***	
A.02		***Necesidad de ofertar Solución completa e integrada***	En los casos de las soluciones que necesitan funcionar de manera coordinadas y/o integradas, se deben incluir y describir explícitamente todos los componentes de hardware, software, suscripciones, servicios, soporte y cualquier otro elemento que sea necesario para que estas soluciones funcionen adecuadamente. En sentido general, el requerimiento obligatorio es que todas las soluciones requeridas sean instaladas y configuradas de manera tal que se cumplan los objetivos de protección y seguridad de los elementos pertinentes, en un formato llave en mano que incluya todos los elementos necesarios para su puesta en funcionamiento total. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra.
A.03		***Todas las soluciones deben ser ofertadas en diseño operacional***	Todas las soluciones ofertadas en este lote deben incluir y describir explícitamente configuraciones con redundancia de alta disponibilidad en las mismas y con cero tolerancia ante un failover. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra.

		de alta disponibilidad	
A.04		***Instalación, Configuración y Puesta a Punto de las soluciones ofertadas***	Deben incluirse y describirse explícitamente todos los servicios, materiales, viáticos y similares necesarios para la instalación, configuración y puesta a punto de todas las soluciones ofertadas en este lote. En los casos de que varias soluciones deban funcionar de forma integrada o coordinada, también deben incluirse todos los servicios, materiales, viáticos y similares necesarios para esas integraciones. Estos servicios deben ser provistos por personal con el nivel de conocimiento adecuado.
			El oferente debe contar con un minimo de 3 ingeniero experto certificado en la solucion y avalados por el fabrcante, es requerido evidenciar dicha certificacion.
A.05		***Certificiaciones***	El oferente debe contar con un minimo de 3 ingenieros expertos certificados en la solucion y avalados por el fabrcante, es requerido evidenciar dicha certificacion.
A.06		***Experiencia del Oferente***	La empresa oferente debe tener mas de 15 anos de experiencia en Ciberseguridad.
			Debe evidenciar al menos 4 clientes con posean la solucion.
			La empresa oferente deber presentar una autorizacion del fabricante por medio de una carta oficial.
A.07		***Dimensionamiento General***	Para los fines de dimensionamiento general pertinentes a cada solución propuesta, en caso de ser necesario, se deben licenciar 300 usuarios locales y moviles , 300 dispositivos, debe soportar como minimo 17 Gbps de Tráfico en Firewall 1518B UDP, 2 Gbps VPN AES-128, debe soportar al menos 4 Gbps en IPS y 3.5 Gbps con todos lo motores encendidos en Next Generation Firewall. Este requerimiento tiene precedencia sobre cualquier error y/u omisión de las especificaciones de cada solución si se diese esa situación.
A.08		***Soporte Técnico***	Debe incluirse y describirse explícitamente el Soporte Técnico a todas las soluciones tanto de Hardware como de Software, servicios de suscripción, y cualquier otro elemento necesario en cada una de las soluciones propuestas. Estos soportes deben ser por un tiempo de 2 años a partir de la puesta en marcha de la solución con un tiempo de respuesta de 2 horas 7X24. Este soporte debe incluir tanto el soporte del oferente local, como el soporte oficial del fabricante de cada solución sin costo adicional. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra.

A.09		***Cursos de Formación***	Se deben incluir y describir explícitamente 5 cupos de formación profesional oficiales, válidos para los esquemas de Certificación Profesional de cada uno de los fabricantes, de cada una de las soluciones ofertadas. Estos cursos deben deben incluir toda la documentación y material de soporte de los mismos.
A.10	***1***	***Solución de Gateways de Manejo y Control de Seguridad Integrada redundantes para Firewall, Prevención de Intrusos, Control de Aplicaciones y Filtrado de URL, Anti Virus, Anti BOT, Emulación y Extracción de Amenazas, VPNs Ipsec, Data Loss Prevention y Sandboxing***	Los Gateways de Manejo y Control de Seguridad Integrada redundante debe ser capaz de manejar los siguientes aspectos de seguridad:
A.11			La funcionalidad de Firewall debe realizar Stateful Inspection utilizando análisis granular de las comunicaciones y Application State para dar seguimiento y controlar el flujo en la red.
A.12			Debe ser capaz de soportar, estar configurada y licenciada para un throughput a la velocidad de conexión agregada hacia Internet de mínimo 250 Mbps con capacidad de crecimiento en el hardware de la solución ofertada a por lo menos el doble de esa velocidad, es decir, hasta un mínimo de 1 Gbps. Debe soportar un Throughput agregado total igual o mayor a 40 Gbps y un mínimo de 4 millones de sesiones concurrentes. Debe tener todas las configuraciones de Hardware y conexiones de red necesarias para manejar estas velocidades. Las conexiones deben ser a 10 Gbps con conectores SFP+ (Por lo menos 4 Puertos), los disco deben ser totalmente integrados en el appliance y la soluccion de tener la capacidad de instalarce en cualquier servidor y funcionar. Debe soportar control de acceso para por lo menos 150 servicios y/o protocolos predefinidos.

A.13			Debe permitir definir reglas de seguridad que puedan ser enforzadas dentro de intervalos de tiempo configurados con tiempo y fecha de expiración. Debe manejar estadísticas de conteo de la utilización de cada una de las reglas de seguridad y enviar las mismas a la aplicación de gerencia de la aplicación.
A.14			Debe soportar métodos de autenticación basados en clientes, usuarios y sesiones.
A.15			La comunicación entre los servidores de gerencia y los Gateways de Seguridad deben ser encriptados y autenticados con Certificados PKI
A.16			Debe soportar DCHP, server y relay. Debe incluir una base de datos de usuarios local que permita la autenticación y autorización sin necesidad de ningún dispositivo externo.
A.17			Deben soportarse los siguientes esquemas de autenticación de usuarios: Tokens (SecureID), TACACS, RADIUS y Certificados Digitales
A.18			Debe soportar y estar configurada en Alta Disponibilidad en los Gateways con balanceo de carga y sincronización de estado. Debe ser capaz de trabajar en modo Bridge/Transparente y soportar HTTP y proxy PTTPS
A.19			Debe soportar la configuración de Cluster N+1, que se pueda tene un cluster hasta de 4 miembros.
A.20			Debe soportar tráfico IPv6 en los módulos de IPS, APP, Firewall, Identity Awareness, filtrado URL, Antivirus y Anti BOT. Debe soportar NAT 6 a 4, o túneles 6 a 4. Debe soportar integración AD usando tráfico IPv6
A.21			Debe soportar seguimiento y logs que muestren el tráfico IPv6. Debe soportar la habilidad de mostrar tablas de ruteo IPv6.
A.22			La solución debe soportar los siguientes RFCs IPv6:
A.23			RFC 1981 Path Maximum Transmission Unit Discovery for IPv6
A.24			RFC 2460 IPv6 Basic specification
A.25			RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
A.26			RFC 3596 DNS Extensions to support IPv6
A.27			RFC 4007 IPv6 Scoped Address Architecture
A.28			RFC 4193 Unique Local IPv6 Unicast Addresses
A.29			RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.
A.30			RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884)
A.31			RFC 4443 ICMPv6

A.32			RFC 4861 Neighbor Discovery
A.33			RFC 4862 IPv6 Stateless Address Auto-configuration
A.34			La solución de IPS debe mínimamente permitir los mecanismos de detección basados en exploit signatures, anomalías de protocolos, y detección por el control y el comportamiento de las aplicaciones
A.35			La solución debe pertenecer al cuadrante de líderes del Cuadrante Mágico de Gartner para las soluciones de Firewall por los menos los ultimos 10 anos.
A.36			Las soluciones de IPS y de Firewall deben estar integradas en una única plataforma
A.37			La administración de la solución de IPS debe permitir que se configure la inspección para proteger solamente los hosts internos. El IPS debe tener las opciones de crear perfiles para protección de clientes, servidores o una combinación de ambos.
A.38			La solución de IPS debe proveer pre configurada por lo menos dos perfiles y/o políticas que puedan ser usadas de forma inmediata
A.39			Los IPS deben tener un mecanismo basado en fail-open que pueda ser configurado en base a límites del uso de la memoria y los CPUs de los Gateways
A.40			Los IPS deben ser capaces de activar o manejar mecanismos automáticos de nuevas firmas desde las actualizaciones. Deben soportar excepciones de redes basadas en la fuente, el destino, el servicio o una combinación de las tres anteriores.
A.41			Los IPS deben incluir una modalidad de Troubleshooting que permita al perfil en uso que solo detecte sin modificar las protecciones individuales
A.42			La solución de IPS debe tener un mecanismo centralizado de correlación y reporte de eventos. El administrador debe ser capaz de activar automáticamente nuevas protecciones basadas en parámetros configurables tales como impacto de rendimiento, severidad de las amenazas, niveles de confianza, protecciones a los clientes y protecciones a los servidores.
A.43			La solución de IPS debe se capaz de detectar y prevenir las amenazas siguientes: Mal uso de protocolos, comunicaciones de Malware, intentos de uso de túneles, y tipos de ataques genéricos sin firmas predeterminadas. Para cada protección, la solución debe incluir tipos de protección para clientes y servidores, severidad de las amenazas, impacto en el rendimiento, niveles de confianza y referencias de la industria.
A.44			Los IPS deben ser capaces de recolectar capturas de paquetes para protecciones específicas. Deben ser capaces de detectar y bloquear ataques a niveles de red y de aplicaciones, protegiendo un mínimo de los siguientes servicios: email, DNS,

			FTP, y Servicios de Windows (Microsoft Networking). La solución debe ser líder protegiendo las vulnerabilidades de Microsoft
A.45			Los IPS y los controles de aplicaciones deben incluir la habilidad para detectar y bloquear aplicaciones P2P y evasivas. El administrador debe ser capaz de definir las redes y los hosts a ser excluidos de la inspección de los IPS
A.46			Los IPS deben proteger del Envenenamiento del Cache del DNS y prevenir a los usuarios de accesar las direcciones de dominios bloqueados. Debe proveer protección a los protocolos de VOIP
A.47			Los IPS y los controles de aplicaciones deben detectar y bloquear las aplicaciones de control remoto, incluyendo aquellas que son capaces de manejar túneles sobre tráfico HTTP. Deben incluir protección a protocolos SCADA y tener un mecanismo para convertir firmas SNORT.
A.48			La solución debe poder enforzar los protocolos de Citrix. Debe permitir al administrador a bloquear fácilmente el tráfico outbound o inbound basado en los Paises, sin necesidad de manejar manualmente rangos de direcciones IP correspondientes a esos países.
A.49			La solución de Adquisición de la Identidad del Usuario debe ser capaz de adquirir la identidad del usuario solicitando la misma al Microsoft Active Directory basada en los eventos de seguridad
A.50			Debe ofrecer un método de Autenticación de Identidad de Usuario basado en browser para los usuarios o activos que no pertenecen a dominio. Debe tener un agente de cliente dedicado que pueda ser instalado por políticas en las computadoras de los usuarios que puedan adquirir y reportar las identidades a los Gateways de Seguridad
A.51			Debe soportar ambientes de terminal servers. Debe integrarse de forma nativa con servicios de directorios, IF-MAP y RADIUS
A.52			El impacto de estos servicios debe ser menor al 3% en los controladores de dominio. La solución debe soportar terminales y servidores Citrix
A.53			La solución debe permitir la identificación a través de un proxy. Debe ser capaz de adquirir la identidad del usuario del Microsoft Active Directory sin necesidad de instalar ningún agente en los controladores de dominio.
A.54			Debe soportar autenticación transparente de Kerberos mediante un sign on único. Debe soportar el uso de grupos anidados de LDAP. Debe ser capaz de compartir y propagar identidades de usuarios entre múltiples gateways de seguridad y crear roles de identidad que puedan ser usados a través de todas las aplicaciones de seguridad

A.55			La base de datos de la Solución para Control de Aplicaciones y Filtrado de URL debe contener más de 8,500 aplicaciones conocidas. Debe tener una categorización de URLs que contenga mas de 200 millones de URLs y unas 240,000 social network widget.
A.56			La solución debe ser capaz de crear reglas de filtrado con múltiples categorías y poder hacer convinacion con otra reglas de firewalls de modo condicional por capas.
A.57			Debe tener granularidad de usuarios y grupos para las reglas de seguridad.
A.58			Los Caches locales de los Gateways de Seguridad deben ser capaces de ofrecer respuestas al 99% de los requerimientos de categorizaciones de los URLs dentro de las primeras 4 semanas luego de la entrada en producción de los mismos
A.59			Debe poseer un interfase fácil, que permita búsquedas para las aplicaciones y los URLs. La solución debe ser capaz de categorizar las aplicaciones y los URLs en base a Factores de Riesgo. El control de las aplicaciones y las políticas de seguridad de los URLF debe ser capaz de ser definido en base a las identidades de los usuarios.
A.60			El control de las aplicaciones y la base de datos de URLF debe ser capaz de ser actualizados mediante servicios en la nube. Debe poder manejar reglas unificadas para el control de aplicaciones y de URLF
A.61			La solución debe proveer mecanismos para informar o preguntar a los usuarios en tiempo real para educarlos o confirmar acciones basadas en las políticas de seguridad.
A.62			La solución debe ser capaz de proveer un mecanismo para limitar el uso de aplicaciones basado en el consumo de ancho de banda de las mismas. Debe permitir excepciones de redes basadas en objetos de redes definidos.
A.63			La Solución debe proveer opciones de modificar la Notificación de Bloqueo y re direccionar al usuario a una página de remediación. Debe incluir mecanismos de Listas Blancas y Negras, y permitir al administrador negar o permitir acceso a URLs específicas independientemente de las categorías.
A.64			La solución debe tener mecanismos configurables de Bypass. Debe proveer un mecanismo de override para la categorización de la base de datos de URLS.
A.65			El control de las aplicaciones y las políticas de seguridad de los URLF deben reportar el conteo de usos de las reglas
A.66			La solución debe incluir las aplicaciones de Anti-BOT y Anti-Virus integradas en los Gateways de Seguridad.

A.67			La aplicación de Anti-BOT debe ser capaz de detectar y detener comportamientos anormales o sospechosos de la red. Debe utilizar un motor de detección de multi-niveles que incluya la reputación de las direcciones Ips, los URLs y las Direcciones de DNS y que detecte patrones de comunicaciones de BOTs. Las protecciones Anti-BOT deben ser capaces de realizar búsquedas de acciones de BOT.
A.68			La solución debe soportar la detección y prevención de virus tipo Cryptors y Ransomware y sus variantes mediante análisis dinámicos y/o estáticos. Debe ser capaz de proteger contra ataques tipo spear phishing.
A.69			Debe poseer capacidades de detección y prevención de C&C DNS hide outs. Debe ser capaz de determinar patrones de tráfico C&C, no solo en su destino de DNS
A.70			Debe ser capaz de realizar ingeniería de reversa para descubrir su DGA (Domain Name Generation). Debe poseer características para manejar traps de DNS para la prevención de amenazas y asistencia en el descubrimiento de hosts infectados que generan comunicaciones C&C. Debe tener capacidades de detección y prevención para proteger de ataques mediante túneles de DNS
A.71			Las políticas de Anti-BOT y Anti-Virus deben poder administrarse desde una consola central. Las aplicaciones de Anti-BOT y Anti-Virus deben tener un mecanismo centralizado de correlación y reportes de eventos.
A.72			La aplicación de Anti-Virus debe ser capaz de prevenir acceso a websites maliciosos e inspeccionar tráfico SSL encriptado. Debe ser capaz de detener archivos maliciosos de entrada. Debe poder escanear archivos almacenados.
A.73			Las soluciones de Anti-BOT y Anti-Virus deben recibir actualizaciones en tiempo real de servicios de reputación basados en la nube. Deben ser capaces de manejar políticas de configuración y enforzamiento granulares de manera centralizada.
A.74			El Anti-Virus debe soportar poder realizar consulta a bases de datos dinamicas en la nube en tiempo real y sin causar latencia.
A.75			La solución debe incluir la Inspección SSL tanto de tráfico entrante como saliente. Debe soportar la Inspección/Decriptamiento con rendimiento líder a través de todas las tecnologías de mitigación
A.76			Debe soportar Perfect Forward Secrecy (PFS, ECDHE conjuntos de cifrado), y AES-NI, AES-GCM para mejoras en el flujo
A.77			Deben incluirse funcionalidades para la emulación de amenazas y sandboxing integradas a la inspección de SSL.
A.78			La solución debe aprovechar la base de datos de filtrado de URLs para permitirle al administrador crear políticas de

			inspección de URLs granulares. Debe ser capaz de inspeccionar filtrado de URLs basado en HTTPS sin requerir decripción SSL
A.79			La solución debe ofrecer la funcionalidad de coordinación e integración con soluciones de Emulación de Amenazas (Sandboxing).
A.80			Debe proveer la habilidad de proteger contra ataques de malware y Zero-Day antes de que las protecciones de firmas estáticas hayan sido creadas. Deben proveer prevención en tiempo real de malware de Paciente-0 en Web Browsing y email
A.81			La Solución de Seguridad debe ser una arquitectura de prevención de amenazas completa y multinivel con mínimo de funcionalidades de: FW, IPS, AV, AB, URLF, APP FW
A.82			La Solución de Seguridad debe soportar emulación de amenazas basada en Redes y Hosts. Debe ser capaz de soportar implementaciones basadas en sitio y en la nube. Se debe incluir en esta propuesta la integración con una solución basada en hosts locales instalados en las premisas de la institución
A.83			La solución debe soportar integración de terceros mediante APIs públicos. Debe soportar implementación en modo Inline, MTA (Mail Transfer Agent), inspect TLS y SSL. Debe soportar implementación en modo de puerto TAP/SPAN
A.84			La solución no debe requerir infraestructura separada para protección de email y protección de WEB.
A.85			Los dispositivos deben soportar instalación en Clusters de alta disponibilidad y deben estar configurados y ofertados en este esquema
A.86			La solución debe ser capaz de emular archivos almacenados ejecutables, documentos JAVA y FLASH, específicamente: 7z, cab,csv,doc, docm, docx,dot,dotm, exe, jar, pdf, potx,pps, ppsm, ppsx, ppt, pptm, pptx,rar, rtf, scr,swf,tar, xla,xls,xlsb, xlsm,xlsx,xlt,xltm,xltx,xlw,zip,pif,com,gz,bz2,tgz,apk,ipa,ISO,js,cpl,vbs,jse,vba,bve,wsf,wsh
A.87			La solución debe ser capaz de emular ejecutables, archivos almacenados, documentos, JAVA y Flash específicamente dentro de los siguientes protocolos: HTTP,HTTPS,FTP,SMTP,CIFS(SMB), SMTP TLS
A.88			El motor de emulación debe soportar múltiples sistemas operativosDE MMicrosoft a 32/64 gbits incluyendo imágenes customizadas. La solución debe ofrecer el soporte de licencias prepopuladas de copias de imágenes Microsoft Windows y Office mediante un acuerdo con Microsoft
A.89			El motor de la solución debe detectar llamados a APIs, cambios en los archivos del sistema, los registros, las conexiones de redes y los procesos del sistema. Debe soportar análisis estático para Windows, mac OS-X, Linux o cualquier plataforma x86

A.90			El motor de emulación de la tecnología de Sandboxing debe ser capaz de inspeccionar, emular, prevenir y compartir los resultados de los eventos de sandboxing en la infraestructura de anti-malware
A.91			La solución debe ser capaz de realizar filtrado estático pre-emulación. La solución debe permitir la emulación de archivos de un tamaño mayor de 10Mb en todos los tipos soportados. Debe soportar motores de detección basados en aprendizaje automático de máquinas.
A.92			La solución debe detectar el ataque en el nivel de explotación, es decir, antes que el código Shell sea ejecutado y antes que el malware sea bajado/ejecutado. Debe ser capaz de detectar los ROP y otras técnicas de explotación tales como escalación de privilegios monitoreando el flujo del CPU
A.93			La solución debe ser capaz de soportar links de escaneo dentro de los emails para malwares desconocidos y de Día0. Debe ser capaz de escanear los URLS históricos almacenados los últimos X días y comprobar si los ratings han cambiado, por ejemplo, de rating limpio a malicioso.
A.94			El tiempo de emulación promedio para determinar un veredicto como benigno no debe tomar más de 1 minuto. El tiempo de emulación promedio para determinar un veredicto de un malware sospechoso como malware no debe tomar más de 3 minutos
A.95			La solución de emulación de amenazas debe permitir Restricciones Geográficas, las cuales permiten que las emulaciones sean restringidas a Países en específico.
A.96			La solución debe proveer la habilidad de incrementar la seguridad compartiendo automáticamente la información de nuevos ataques con otros Gateways utilizando la actualización de firmas entre otros
A.97			El motor de emulación debe exceder un 90% de captura en las pruebas de Virus Totales donde los pdf´s y exe´s son modificados con encabezados ¨no usados¨ para demostrar la capacidad de la solución para detectar malware nuevo y desconocido. La solución debe detectar tráfico C&C de acuerdo la reputación dinámica de los ip/url
A.98			La Solución debe ser capaz de emular y extraer archivos embebidos en documentos. Debe ser capaz de escanear documentos que contengan URLs

A.99			La solución debe monitorear las actividades sospechosas en: Llamadas a APIs, Cambios en archivos del Sistema, Registro del Sistema, Conexiones de redes, Procesos del Sistema, Creación y borrado de archivos, Modificaciones de Archivos, Inyección de código al Kernel, Detección de intentos de escalamiento de privilegios, Modificaciones al Kernel (Cambios de memoria realizados por el código del Kernel, no el hecho de que se cargue un driver, esto esta cubierto por el elemento anterior), Comportamiento del código del Kernel, monitoreo de las actividades de código que no sea modalidad de usuario. Interacción física directa con el CPU, Detección de Bypass del Control de Acceso de Usuario.
A.100			La solución debe poseer capacidades de anti-evasión detectando la ejecución del Sandbox. Debe ser resiliente a casos donde el código shell o el malware puede no ejecutarse si detectan la existencia de un ambiente virtual (Hipervisor propietario). Debe ser resiliente a delays implementados en las etapas del código shell o el malware. Debe ser resiliente a casos donde el código shell o el malware solo se ejecute luego de un reinicio o apagado del end point.
A.101			La solución debe emular actividades de usuarios reales tales como clicks del ratón, uso del teclado, etc. Debe ser capaz de identificar íconos que son similares a documentos de aplicaciones populares. Debe proteger contra evasión dentro de archivos flash (swf)
A.102			La solución debe ofrecer la funcionalidad de poder ser manejada de forma centralizada. Luego de la detección de archivos maliciosos, se debe generar un reporte detallado para cada uno de los archivos maliciosos. El reporte detallado debe incluir capturas de pantallas, líneas de tiempo, las modificaciones o creaciones clave en el registry, la creación de archivos y/o procesos, y la actividad de red detectada
A.103			La solución debe eliminar las amenazas y remover el contenido explotable, incluyendo el contenido activo y los objetos embebidos. Debe ser capaz de reconstruir los archivos con los elementos seguros conocidos. Debe tener la capacidad de convertir los archivos reconstruidos a formato PDF. Debe mantener la flexibilidad de mantener el formato original del archivo y especificar el tipo de contenido que será removido.
A.104			La solución de seguridad de Anti-Spam y Email debe ser agnóstica al lenguaje y al contenido. Debe poseer clasificación y protección en tiempo real basados en la detección de brotes de spam que están basados en patrones y no en contenido. Debe incluir el bloqueo de IPs basados en reputación desde un servicio online para evitar falsos positivos

A.105			Debe incluir mecanismos de protección de Hora Cero para nuevos virus propagados a través de email y spam sin depender solamente en inspección de contenido o heurística
A.106			Para las funcionalidades de Ipsec VPNs debe soportar CA internos y externos de terceros. Debe soportar criptografía 3DES y AES-256 para IKE fase 1 y IIIKEv2 , Suite-B-GCM-128 y Suite B-GCM-256 para fase II.
A.107			Debe soportar por lo menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 y Grupo 20. Debe soportar integridad de Data con md5, sha1SHA-256, SHA-384 y AES-XCBC
A.108			La solución debe soportar VPN sitio a sitio en las siguientes topologías: Full Mesh (all to all), Star (Oficinas remotas con sitio principal), Hub and Spoke (Sitio Remoto a través del Sitio Central con otro Sitio Remoto). Debe soportar la configuración de los VPNs mediante un GUI que permita la adición de objetos a las comunidades de VPNs mediante drag and drop.
A.109			Debe soportar SSL VPN clientless para acceso remoto. Deben soportar VPNs L2TP incluyendo los clientes para Iphones.
A.110			Debe permitir que el administrador aplique las reglas de seguridad para controlar el tráfico dentro de los VPNs. Debe soportar VPNs basados en dominios, y rutas usando protocolos de ruteo dinámico y VTIs. Debe incluir la habilidad de establecer VPNs dentro de gateways con IPs dinámicas públicas y compresión IP para VPNs cliente a sitio y sitio a sitio.
A.111			La aplicación de manejo de seguridad debe soportar cuentas de administradores basadas en roles, ejemplo, un rol solo para establecimiento de las políticas de firewall o un rol solo para visualización. Debe incluir canales de comunicación seguros basados en encripción de Certificados para todas las soluciones de diferentes fabricantes que pertenezcan a un dominio de gerencia.
A.112			La solución debe incluir una Autoridad de Certificados Interna, x509 CA que pueda generar Certificados a gateways y usuarios para permitir un mecanismo eficiente de autenticación en los VPNs. Debe incluir la capacidad de usar CA s externos que soporten estándares PKCS#12, CAPI o ENTRUST
A.113			Todas las aplicaciones de seguridad en este grupo deben ser capaces de ser manejadas desde una consola central. La solución de gerencia debe proveer un conteo de los hits a las reglas de seguridad en las políticas de seguridad. Debe incluir opciones de búsqueda que permitan investigar cual objeto de red contiene una dirección IP específica o una parte de ella.

A.114			Debe incluir la opción de segmentar la base de reglas utilizando etiquetas o títulos de secciones para mejor organización de las políticas. Debe proveer la opción de salvar la política completa o una parte específica de la misma. Debe poseer mecanismos de verificación de políticas de seguridad previo a la instalación de las mismas. Debe poseer mecanismos de control de revisión de las políticas de seguridad.
A.115			La solución debe proveer las opciones de añadir alta disponibilidad a la gerencia de seguridad, usando un servidor de gerencia standby que se sincroniza automáticamente con el servidor activo sin la necesidad de dispositivos externos de almacenamiento. Esta funcionalidad debe ser incluida en las propuestas de la licitación.
A.116			La solución de seguridad debe incluir un mapa comprensivo de todos los objetos de redes y sus conexiones que pueda ser exportado a Microsoft Visio o a un archivo de imágenes.
A.117			Debe incluir la habilidad de distribuir y aplicar de forma centralizada nuevas versiones de software a los diferentes gateways de seguridad. Debe incluir una herramienta de manejo de las licencias de los diferentes gateways de seguridad que debe ser controlada por la estación de gerencia. Debe tener la capacidad de manejo de multi dominios y soportar la funcionalidad de políticas de seguridad globales a través de los dominios.
A.118			El interfase gráfico de la herramienta de gerencia debe tener la habilidad de poder excluir direcciones IP de la definición de firmas de la solución de IPS. Debe tener la capacidad de excluir direcciones IP de los logs de IPS cuando se detectan como falsos positivos. Debe ser capaz de alcanzar las definiciones de firmas de IPS desde los logs de IPS.
A.119			El licitante debe proveer los detalles de sus mecanismos de actualización y de su habilidad para manejar ataques de día cero a través de todas las soluciones de prevención de amenazas incluyendo IPS, Control de Aplicaciones, Filtrado de URL, Anti BOT y anti Virus. Debe proveer los detalles de la categorización de los URLs bajo las circunstancias de que ese website haya sido comprometido y este distribuyendo malware
A.120			El mecanismo de logging central debe ser parte del sistema de administración, los administradores deben tener la capacidad de instalar servidores de almacenamiento de Logs adicionales.
A.121			La operación de logs debe proveer la opción de operar en el servidor de gerencia o en servidores dedicados. Debe ser capaz de operar en servidores X86 abiertos. Se debe entregar la lista de compatibilidad. La solución debe tener la habilidad de almacenar todos los logs para todas las reglas de seguridad. El buscador de logs debe tener la capacidad de realizar búsquedas indexadas.

A.122			La solución debe tener la capacidad de hacer logs a todas las aplicaciones integradas en esta solución, incluyendo IPS, Aplication Control, URL Filtering, Antivirus, AntiBOT, User Identity.
A.123			La solución debe incluir un mecanismo de captura automática de paquetes para los eventos de IPS de forma tal que se puedan realizar mejores análisis forénsicos. Debe proveer diferentes logs para regular las actividades de los usuarios y los relacionados a la gerencia.
A.124			La solución debe proveer para cada ocurrencia de un hit de reglas de seguridad las siguientes opciones: LOG, alerta, trap SNMP, email o la ejecución de un script definido por el usuario. Los LOGs debe tener un canal seguro de comunicaciones para la transferencia de los mismos para evitar escuchas, esta solución debe estar autenticada y encriptada. Los logs deben ser transferidos de manera segura entre el gateway, la gerencia, los servidores dedicados de LOGs y las consolas de visualización en las estaciones de los administradores
A.125			La solución debe incluir la opción de bloquear dinámicamente una conexión activa desde el interfase gráfico del LOG sin necesidad de modificar las bases de reglas. Debe ser capaz de exportar logs en formato de bases de datos. Debe soportar el cambio automático del archivo de LOGs basado en tiempos preestablecidos o en el tamaño de los archivos
A.126			Debe soportar el manejo de excepciones a los enforzamientos IPS desde el record de LOG. Debe ser capaz de asociar un nombre de usuario y un nombre de máquina a cada record de LOG.
A.127			La herramienta de manejo gráfica debe ser capaz de monitorear fácilmente el estatus de los gateways. Esta herramienta debe proveer información del sistema para cada gateway, incluyendo: uso de memoria, CPU, particiones de discos y espacio restante. Debe proveer el status de cada componente del gateway tales como firewall, vpn, clúster, antivirus, etc. Debe incluir el estatus de todos los túneles de VPNs, sitio a sitio y cliente a sitio.
A.128			La solución debe permitir la definición de umbrales y de las acciones a realizar cuando los mismos son alcanzados en los gateways. Las acciones deben incluir: LOGs, Alertas, traps SNMP, email y la ejecución de un script definido por el usuario. Debe incluir gráficos pre configurados para monitorear la evolución en el tiempo del tráfico y de los contadores del sistema: reglas de seguridad máximas, usuarios P2P, túneles VPNs, tráfico de red y otras informaciones útiles. Debe proveer la funcionalidad de generar nuevos gráficos personalizados usando diferentes tipos de tablas.

A.129			La solución debe proveer la capacidad de grabar las vistas de tráfico y de sistemas para visualización futura en cualquier momento. Debe ser capaz de reconocer el mal funcionamiento y los problemas de conectividad entre dos puntos conectados a través de un VPN, y crear logs y realizar alertas cuando un túnel VPN está abajo
A.130			La funcionalidad de correlación de eventos debe estar integrada totalmente en la aplicación de gerencia. Debe incluir herramientas para correlacionar eventos de todas las funcionalidades del gateway y de dispositivos y soluciones de terceros. Debe permitir la creación de filtros basados en cualquier característica de evento tales como aplicaciones de seguridad, direcciones IP origen y destino, servicio, tipo de evento, severidad, nombre del ataque, país de origen y destino, etc. Debe tener un mecanismo de asignación de estos filtros a diferentes gráficos de línea que puedan ser actualizados a intervalos regulares mostrando todos los eventos correspondientes a ese filtro, esto le permite al operador enfocarse en los eventos más importantes.
A.131			La funcionalidad de correlación de eventos debe suministrar una vista gráfica de los eventos basados en tiempo. Debe mostrar la distribución de eventos por países en un mapa. Debe permitir al administrador a agrupar los eventos basados en cualquiera de sus características incluyendo niveles de anidamiento y su exportación en formato PDF.
A.132			La funcionalidad debe incluir la opción de búsqueda dentro de la lista de eventos, y el drill down en los detalles para la investigación y análisis forénsico. Se debe incluir la funcionalidad de la creación de tablas gráficas con las características de los eventos.
A.133			La solución debe ser capaz de detectar ataques de denegación de Servicios correlacionando eventos de todas las fuentes. Debe detectar un login de administrador en horas irregulares. Debe detectar ataques de adivinación de credenciales. La solución debe reportar sobre todas las instalaciones de políticas de seguridad.
A.134			La solución debe incluir reportes predefinidos por hora, día, semana y mes incluyendo por lo menos los Eventos, Fuentes, Destinos, Servicios, Fuentes máximos, Fuentes máximas y sus eventos máximos, Destinos máximos y sus eventos máximos y los servicios máximos y sus eventos máximos. La herramienta de reportes debe permitir la aplicación de por lo menos 25 filtros que permitan personalizar los reportes predefinidos de acuerdo a las necesidades de los administradores

A.135			La herramienta de reportes debe soportar la calendarización automática de los reportes para la información que debe ser extraída de forma regular (día, semana, mes). La solución debe permitir al administrador definir la fecha y hora en que los reportes comienzan a generarse. Debe soportar formatos de reporte HTML, CSV y MHT. Debe soportar la distribución automáticas por email, la subida a servidores FTP/WEB y scripts personalizados de distribución de los mismos.
A.136			El sistema de reportes debe proveer información consolidada sobre: El volumen de conexiones que fueron bloqueadas por reglas de seguridad. Las fuentes máximas de las conexiones bloqueadas, su destino y servicios. Reglas máximas usadas por las políticas de seguridad por los puntos de enforzamiento (perímetro). Servicios de redes máximos. Actividad WEB por usuarios detallando los sitios más visitados y los mayores usuarios. Servicios máximos que crearon la mayor carga para el tráfico encriptado. Usuarios máximos de VPNs que realizan las conexiones de mayor duración.
A.137			La solución debe incluir un Portal de Gerencia con acceso basado en browser para visualizar en modo solo lectura las políticas de seguridad, manejar los logs de los firewalls y usuarios, proveyendo acceso a los gerentes y auditores sin la necesidad de usar la aplicación de gerencia. Esta solución debe incluir soporte SSL y puertos configurables.
A.138			La solución de Seguridad blades de proteccion de Data Loss Prevention (DLP) que debe ser manejada de manera centralizada con las otras aplicaciones de seguridad de esta suite.
A.139	1	***Solución de Sandboxing***	La solución deberá 100% compatible con la plataforma de Correo Office365 y Onpremise. Debe ser capaz de funcionar de forma coordinada e integrada con la Solución de Gateways de Manejo y Control de Seguridad Integrada ofertada en esta licitación.
A.140			La solución debe funcionar en equipos propuestos a ser instalados en las premisas o en la nube, como usted lo recomiende.
A.141			Deberá permitir analizar la ejecución de código malicioso en sistemas operativos virtuales
A.142			Deberá contar con mecanismos que permitan la evaluación del malware en sistemas operativos no virtualizados dentro de la solución
A.143			La solución debe trabajar en modo prevención y no en modo detección; es decir, no se debe permitir el ingreso del malware en zonas de cuarentena, ya que esto implica que se debe permitir el paso de código malicioso a la entidad, para ser examinado de forma posterior. Lo anterior introduce riesgos de propagación de malware.

A.144			Deberá permitir la detección de modificación de Archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red
A.145			Deberá presentar la información completa del análisis de amenazas del ambiente virtual incluyendo Actividades del sistema, acción del exploit, trafico web, intentos de comunicación entre otros
A.146			La solución deberá integrarse con el módulo de URL Filtering propuesto en esta licitación para bloquear los sitios infectados, de mala reputación o reconocidos como Centros de comando y control que puedan manipular maquinas internas y desplegar ataques posteriores.
A.147			La solución deberá estar en la capacidad de procesar múltiples archivos al mismo tiempo, se debe contar con múltiples VM para el análisis de Sandbox OS
A.148			La solución debe tener la capacidad de integrarse en modo MTA y controlar la recepción de correo en modo Seguro utilizando TLS (control SMTP & SMTPS)
A.149			Debe poder funcionar en modo Sniffer o en modo en línea (Bridge o Capa3) controlando la navegación (HTTP, HTTPS) y la transferencia de archivos FTP
A.150			Deberá permitir que los archivos que son analizados con el OS Sandbox deben entregar un análisis posterior a la ejecución de las siguientes características:
A.151			Descarga de Virus
A.152			Modificación de Registro
A.153			Conexiones externas a Ips maliciosas
A.154			Infección de procesos
A.155			La solución debe permitir la emulación de tamaño de archivos de más de 15 Mb
A.156			La solución debe ser capaz de detectar ROP y otras técnicas de explotación (por ejemplo escalamiento de privilegios) controlando el flujo de CPU
A.157			La solución debe tener capacidades anti-evasión detección ejecución caja de arena(sandboxing)
A.158			El motor de emulación debe tener la capacidad de detección anti-virtual machine
A.159			Solución debe ser resistente a los casos en que el malware ejecute un reinicio o un apagado de la máquina virtual de Sandboxing
A.160			La solución debe emular las actividades reales de los usuarios, tales como clics del ratón, pulsaciones de teclas, etc

A.161			La solución debe eliminar las amenazas y eliminar contenido explotable, incluyendo el contenido activo y objetos incrustados
A.162			La solución debe ser capaz de reconstruir los archivos con los elementos de seguridad conocidos
A.163			La solución debe proporcionar capacidad de convertir archivos reconstruidos a formato PDF
A.164			La solución debe mantener la flexibilidad con posibilidad y la opción de mantener el formato de archivo original y especificar el tipo de contenido que será eliminado.
A.165			Solución debe ser resistente a los retrasos implementados en el código shell o etapas de malware.
A.166			Solución debe ser resistente a los casos en que el código shell o malware ejecutarían sólo de un reinicio o un apagado del punto final.
A.167			La Solución debe ser resistente a los casos en que el código shell o malware no se ejecutarán si detectan la existencia de entornos virtuales.
A.168			Las soluciones de Hardware deben ser ofertadas en clusters de alta disponibilidad con fuentes de poder y abanicos redundantes.
A.169		***Proteccion Avanzada de Malware***	La solucion debe se manejada de manera cenralizada y que permita la definicion de politicas y la creacion de grupos de sistemas o usuarios.
A.170			La solucion debe ser capaz de definir white list para realizar excepciones.
A.171			La solucion debe tener API para fines de integraciones
A.172			La solucion debe proveer roles de acceso a la consola.
A.173			La solucion debe proveer control granular de Device Control
A.174			La solucion debe soportar Sistemas Operativos tales como Windows 7 SP1 Pro & Enterprise & higher; Windows 2008 R2 +; Mac OS 10.13 & 10.14, VDI. Linux
A.175			LA solucion no debe consumir para de un 2% de CPU y no mas de 300MB de RAM en funcionamiento normal.
A.176			La solucion debe incluir EDR (Endpoint Detection and Response)
A.177			El EDR de la solucion de funcionar en tiempo real sin importar la locacion del usuario.
A.178			La solucion debe proveer reporte en formatos concidos(xlm, cvs, pdf)
A.179			La solucion debe proveer reporte de analisis forence.
A.180			Los reporte debe tener la capacidad de realizar envio automatico bajo calendarizacion.

A.181			Debe colectar eventos con fines de investigacion forence del tipo: - process events - file creation, any accesss, modification, copy, delete, rename - registry access or modifications - network connections - http/URL access - cross-process activity (e.g. mutexes ...) - command line arguments - windows events - DNS queries and responses - user logons - process injections
A.182			Realizar analisis forence usando tecnicas de MITRE ATT&CK (tácticas, técnicas y conocimiento común de adversarios)
A.183			Debe ser capaz de detectar y prevenir comportamiento malicioso tales como: Levantamiento de proceso de forma anormal, Creacion de archivos armales, copia de archivos anormales, Eliminar archivos, ejecucion de procesos anormales, Cambios de privilegios de forma anormal, Eliminacion de Shadow Copy de forma normal
A.184			Capacidad de responder a un atanque de dia cero de forma automatica sin ser un pasciente cero.
A.185			capacidad de realizar rollback a todo los proceso de encripcion de ransomware de dia cero aun sin tener contacto con el sandbox
A.186			La solucion debe tener capacidad de proteccion de antiphising a nivel de endppoint, debe tomar accion y proteger el ususario final de no colocar informaciones personales tales como: Nombre, Apellido, Numero de tarjeta de credito, cedula, etc.
A.187			La solucion debe tener capacidad de integrarse con Office365 y realizar protecciones avanzadas.
A.188			La solucion debe proteger de phishing, malware, ataque de dia cero, spam, a nivel del office365.
A.189			La solucion debe brindar informacion y unalisis que explique el porque algun archivo o email es catalogado como maliciosos.
A.190			Se requiere que la solucion brinde visibilidad de la ubicacion geografica de los logins de los usuarios.

Consideraciones adicionales:

1. El envío de una Propuesta no implica un compromiso directo del MINC con el oferente.

2. El MINC se reserva el derecho de elegir como la mejor propuesta, de manera completa o parcial, aquella que mejor represente los objetivos del negocio.
3. Las especificaciones incluidas en la presente solicitud suponen configuraciones mínimas deseadas, en tal sentido se considerará un valor agregado que los suplidores opten por presentar alternativas superiores que compitan en precio con lo aquí especificado.
4. El modelo a ofertar debe ser para servicios de Seguridad Perimetral y Protección Avanzada de Antimalware.
5. La contratación se realizará por un (1) año.

Se efectuará la evaluación técnica de las ofertas considerando los siguientes aspectos:

A. Experiencia del Oferente y Personal

- Experiencia de la empresa en el mercado.
- Prestación de servicios similares en otras empresas o instituciones estatales.

B. Calidad de la propuesta técnica en la metodología y gestión del proyecto

- Tiempo de crédito otorgado a la Entidad Contratante.

2.1 Criterio de Evaluación

Las Propuestas deberán contener la documentación necesaria, suficiente y fehaciente para demostrar los siguientes aspectos que serán verificados bajo la modalidad "CUMPLE/ NO CUMPLE";

Elegibilidad: Que el Proponente está legalmente autorizado para realizar sus actividades comerciales en el país, y satisface todos los requisitos exigidos.

Capacidad Técnica: Que los Bienes cumplan con todas las características especificadas en las Fichas Técnicas.

2.2 Fase de Homologación

Cada oferente deberá incluir en el formulario de presentación de muestra de certificados, sellos, sobres.

Una vez concluida la recepción de los "Sobres A", se procederá a la ponderación de la documentación solicitada y a la validación de las ofertas conforme a los términos de referencia requeridos, bajo la modalidad "CUMPLE/ NO CUMPLE".

Los Peritos levantarán un informe donde se indicará el cumplimiento o no de los Pliegos de Condiciones Específicas. En el caso de no cumplimiento indicará, de forma individualizada las razones.

Los Peritos emitirán su informe al Comité de Compras y Contrataciones sobre los resultados de la evaluación de las Propuestas Técnicas "Sobre A", a los fines de la recomendación final.

2.3 Evaluación económica

El Comité de Compras y Contrataciones evaluará y comprará únicamente las Ofertas que se ajustan sustancialmente al presente Pliego de Condiciones Específicas y que hayan sido evaluadas técnicamente como CONFORME, bajo el criterio del mejor precio ofertado, experiencia v calidad.