REPÚBLICA DOMINICANA

MINISTERIO DE HACIENDA

"Año del Desarrollo Agroforestal"

PLIEGO DE CONDICIONES ESPECÍFICAS PARA COMPRA DE BIENES Y SERVICIOS CONEXOS

Contratación de empresas para actualización y adecuación del Centro de Datos, donde se albergará el sistema para el control de las operaciones de los establecimientos de juegos y apuestas de la Dirección de Casinos y Juegos de Azar del Ministerio de Hacienda, 2da convocatoria.

Licitación Pública Nacional
MH-CCC-LPN- 2017-0010

Santo Domingo, Distrito Nacional
República Dominicana
Noviembre 2017

TABLA DE CONTENIDO

GENERALIDADES

Prefacio

Este modelo estándar de Pliego de Condiciones Específicas para Compras y Contrataciones de Bienes y/o Servicios conexos, ha sido elaborado por la Dirección General de Contrataciones Públicas, para ser utilizado en los Procedimientos de Licitaciones regidos por la Ley No. 340-06, de fecha dieciocho (18) de agosto del dos mil seis (2006), sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, su modificatoria contenida en la Ley No. 449-06, de fecha seis (06) de diciembre del dos mil seis (2006), y su Reglamento de Aplicación emitido mediante el Decreto No. 543-12 de fecha seis (6) de septiembre de dos mil doce (2012).

A continuación se incluye una breve descripción de su contenido.

PARTE 1 – PROCEDIMIENTOS DE LICITACIÓN

Sección I. Instrucciones a los Oferentes (IAO)

Esta sección proporciona información para asistir a los Oferentes en la preparación de sus Ofertas. También incluye información sobre la presentación, apertura y evaluación de las ofertas y la adjudicación de los contratos. Las disposiciones de la Sección I son de uso estándar y obligatorio en todos los procedimientos de Licitación para Compras y Contrataciones de Bienes y/o Servicios conexos regidos por la Ley No. 340-06 sobre Compras y Contrataciones con modificaciones de Ley No. 449-06 y su Reglamento de aplicación aprobado mediante Decreto No. 543-12.

Sección II. Datos de la Licitación (DDL)

Esta sección contiene disposiciones específicas para cada Compra y Contratación de Bienes y/o Servicios conexos, y complementa la Sección I, Instrucciones a los Oferentes.

Sección III. Apertura y Validación de Ofertas

Esta sección incluye el procedimiento de apertura y validación de Ofertas, Técnicas y Económicas, incluye los criterios de evaluación y el procedimiento de Estudio de Precios.

Sección IV. Adjudicación

Esta sección incluye los Criterios de Adjudicación y el Procedimiento para Adjudicaciones Posteriores.

PARTE 2 - CONTRATO

Sección V. Disposiciones sobre los Contrato

Esta sección incluye el Contrato, el cual, una vez perfeccionado no deberá ser modificado, salvo los aspectos a incluir de las correcciones o modificaciones que se hubiesen hecho a la oferta seleccionada y que están permitidas bajo las Instrucciones a los Oferentes y las Condiciones Generales del Contrato.

Incluye las cláusulas generales y específicas que deberán incluirse en todos los contratos.

PARTE 3 – ENTREGA Y RECEPCIÓN

Sección VI. Recepción de los Productos

Esta sección incluye los requisitos de la entrega, la recepción provisional y definitiva de los bienes, así como las obligaciones del proveedor.

Sección VII. Formularios

Esta sección contiene los formularios de información sobre el oferente, presentación de oferta y garantías que el oferente deberá presentar conjuntamente con la oferta.

PARTE I
PROCEDIMIENTOS DE LA LICITACIÓN

Sección I
Instrucciones a los Oferentes (IAO)

1.1 Antecedentes

Desde la promulgación de la Ley No. 494-06, de fecha 27 de diciembre de 2006, de Organización de la Secretaría de Estado de Hacienda, hoy Ministerio de Hacienda, todas las competencias administrativas y de control de las operaciones de los juegos de azar, han sido concentradas en el Ministerio de Hacienda (MH). No obstante, no fue hasta los años 2011 y 2012 en virtud de lo establecido en la Ley No. 253-12, de fecha 9 de noviembre de 2012, sobre el Fortalecimiento de la Capacidad Recaudatoria del Estado para la Sostenibilidad Fiscal y el Desarrollo Sostenible, que se hizo efectivo el traspaso del control de las operaciones de Bancas de Apuestas Deportivas, Bingos y Bancas de Lotería hacia la Dirección de Casinos y Juegos de Azar del MH.

En la actualidad se cuenta con un total siete (7) leyes y un (1) reglamento de aplicación, que regulan los temas técnicos de algunos de los establecimientos de juegos, tales como: Casinos, Bancas de apuestas deportivas y la instalación de máquinas tragamonedas.

Es por ello que la Dirección de Casinos y Juegos de Azar del MH, en su rol de órgano regulador de los juegos de azar, presentó el proyecto "Fortalecimiento de Control y Supervisión de Operaciones de Bancas y Casinos".

Entre los objetivos del referido proyecto se destaca el de "Establecer un sistema eficiente para el control de las operaciones de los establecimientos de juegos y apuestas en la Republica Dominicana", para lograrlo se planteó el diseño e implementación de una herramienta informática para el registro y control de las operaciones de los juegos. Dicha herramienta tendría que estar soportada sobre una infraestructura en términos de Centro de Datos, capaz de garantizar la seguridad de la información y la disponibilidad de los servicios, así como una plataforma tecnológica escalable y segura.

Por todo lo antes expuesto, se estableció para el primer año de ejecución, el fortalecimiento y la readecuación del Centro de Datos del MH, el cual servirá para albergar dicho sistema.

1.2 Objetivos y Alcance

El objetivo del presente documento es establecer el conjunto de cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, por el que se fijan los requisitos, exigencias, facultades, derechos y obligaciones de las personas naturales o jurídicas, nacionales o extranjeras, que deseen participar en la **"Contratación de empresas para actualización y adecuación del Centro de Datos, donde se albergará el sistema para el control de las operaciones de los establecimientos de juegos y apuestas de la Dirección de Casinos y Juegos de Azar del Ministerio de Hacienda, 2da Convocatoria",** llevada a cabo por **el MINISTERIO DE HACIENDA (Referencia: MH-CCC-LPN- 2017-0010.**

Este documento constituye la base para la preparación de las Ofertas. Si el Oferente/Proponente omite suministrar alguna parte de la información requerida en el presente Pliego de Condiciones Específicas o presenta una información que no se ajuste sustancialmente en todos sus aspectos al mismo, el riesgo estará a su cargo y el resultado podrá ser el rechazo de su Propuesta.

1.3 Definiciones e Interpretaciones

A los efectos de este Pliego de Condiciones Específicas, las palabras y expresiones que se inician con letra mayúscula y que se citan a continuación tienen el siguiente significado:

Adjudicatario: Oferente/Proponente a quien se le adjudica el Contrato u Orden de Compra.

Bienes: Productos elaborados a partir de materias primas, consumibles para el funcionamiento de los Entes Estatales.

Caso Fortuito: Acontecimiento que no ha podido preverse, o que previsto no ha podido evitarse, por ser extraño a la voluntad de las personas.

Circular: Aclaración que el Comité de Compras y Contrataciones emite de oficio o para dar respuesta a las consultas planteadas por los Oferentes/Proponentes con relación al contenido del Pliego de Condiciones, formularios, otra Circular o anexos, y que se hace de conocimiento de todos los Oferentes/Proponentes.

Comité de Compras y Contrataciones: Órgano Administrativo de carácter permanente responsable de la designación de los peritos que elaborarán las especificaciones técnicas del bien a adquirir y del servicio u obra a contratar, la aprobación de los Pliegos de Condiciones Específicas, del Procedimiento de Selección y el dictamen emitido por los peritos designados para evaluar ofertas.

Compromiso de Confidencialidad: Documento suscrito por el Oferente/Proponente para recibir información de la Licitación.

Consorcio: Uniones temporales de empresas que sin constituir una nueva persona jurídica se organizan para participar en un procedimiento de contratación.

Consulta: Comunicación escrita, remitida por un Oferente/Proponente conforme al procedimiento establecido y recibida por el Comité de Compras y Contrataciones, solicitando aclaración, interpretación o modificación sobre aspectos relacionados exclusivamente con el Pliego de Condiciones Específicas.

Contrato: Documento suscrito entre la institución y el Adjudicatario elaborado de conformidad con los requerimientos establecidos en el Pliego de Condiciones Específicas y en la Ley.

Credenciales: Documentos que demuestran las calificaciones profesionales y técnicas de un Oferente/Proponente, presentados como parte de la Oferta Técnica y en la forma establecida en el Pliego de Condiciones Específicas, para ser evaluados y calificados por los peritos, lo que posteriormente pasa a la aprobación del Comité de Compras y Contrataciones de la entidad

contratante, con el fin de seleccionar los Proponentes Habilitados, para la apertura de su Oferta Económica Sobre B.

Cronograma de Actividades: Cronología del Proceso de Licitación.

Día: Significa días calendarios.

Días Hábiles: Significa día sin contar los sábados, domingos ni días feriados.

Enmienda: Comunicación escrita, emitida por el Comité de Compras y Contrataciones, con el fin de modificar el contenido del Pliego de Condiciones Específicas, formularios, anexos u otra Enmienda y que se hace de conocimiento de todos los Oferentes/Proponentes.

Entidad Contratante: El organismo, órgano o dependencia del sector público, del ámbito de aplicación de la Ley No. 340-06, que ha llevado a cabo un proceso contractual y celebra un Contrato.

Estado: Estado Dominicano.

Fichas Técnicas: Documentos contentivos de las Especificaciones Técnicas requeridas por la Entidad Contratante.

Fuerza Mayor: Cualquier evento o situación que escapen al control de la Entidad Contratante, imprevisible e inevitable, y sin que esté envuelta su negligencia o falta, como son, a manera enunciativa pero no limitativa, epidemias, guerras, actos de terroristas, huelgas, fuegos, explosiones, temblores de tierra, catástrofes, inundaciones y otras perturbaciones ambientales mayores, condiciones severas e inusuales del tiempo.

Interesado: Cualquier persona natural o jurídica que tenga interés en cualquier procedimiento de compras que se esté llevando a cabo.

Licitación Pública: Es el procedimiento administrativo mediante el cual las entidades del Estado realizan un llamado público y abierto, convocando a los interesados para que formulen propuestas, de entre las cuales seleccionará la más conveniente conforme a los Pliegos de Condiciones correspondientes. Las licitaciones públicas podrán ser internacionales o nacionales. La licitación pública nacional va dirigida a los Proveedores nacionales o extranjeros domiciliados legalmente en el país.

Licitación Restringida: Es la invitación a participar a un número limitado de proveedores que pueden atender el requerimiento, debido a la especialidad de los bienes a adquirirse, razón por la cual sólo puede obtenerse un número limitado de participantes, de los cuales se invitará un mínimo de **cinco (5) Oferentes** cuando el registro sea mayor. No obstante ser una licitación restringida se hará de conocimiento público por los medios previstos.

Líder del Consorcio: Persona natural o jurídica del Consorcio que ha sido designada como tal.

Máxima Autoridad Ejecutiva: El titular o el representante legal de la Entidad Contratante o quien tenga la autorización para celebrar Contrato.

Notificación de la Adjudicación: Notificación escrita al Adjudicatario y a los demás participantes sobre los resultados finales del Procedimiento de Licitación, dentro de un plazo de **cinco (05) días hábiles** contados a partir del Acto de Adjudicación.

Oferta Económica: Precio fijado por el Oferente en su Propuesta.

Oferta Técnica: Especificaciones de carácter técnico-legal de los bienes a ser adquiridos.

Oferente/Proponente: Persona natural o jurídica legalmente capacitada para participar en el proceso de compra.

Oferente/Proponente Habilitado: Aquel que participa en el proceso de Licitación y resulta Conforme en la fase de Evaluación Técnica del Proceso.

Peritos: Funcionarios expertos en la materia del proceso llevado a cabo, de la Entidad Contratante, de otra entidad pública o contratados para el efecto y que colaborarán asesorando, analizando y evaluando propuestas, confeccionando los informes que contengan los resultados y sirvan de sustento para las decisiones que deba adoptar el Comité de Compras y Contrataciones.

Prácticas de Colusión: Es un acuerdo entre dos o más partes, diseñado para obtener un propósito impropio, incluyendo el influenciar inapropiadamente la actuación de otra parte.

Prácticas Coercitivas: Es dañar o perjudicar, o amenazar con dañar o perjudicar directa o indirectamente a cualquier parte, o a sus propiedades para influenciar inapropiadamente la actuación de una parte.

Prácticas Obstructivas: Es destruir, falsificar, alterar u ocultar en forma deliberada pruebas importantes respecto de su participación en un proceso de compra o incidir en la investigación o formular declaraciones farsas a los investigadores con la intensión de impedir sustancialmente una investigación de la Entidad Contratante referente a acusaciones sobre prácticas corruptas, fraudulentas, coercitivas, o colusorias y/o amenazar, acosar o intimidar a una parte con el propósito de impedir que dicha parte revele lo que sabe acerca de asuntos pertinentes a la investigación, o que lleve adelante la investigación, o la ejecución de un Contrato.

Pliego de Condiciones Específicas: Documento que contiene todas las condiciones por las que habrán de regirse las partes en la presente Licitación.

Proveedor: Oferente/Proponente que habiendo participado en la Licitación Pública, resulta adjudicatario del contrato y suministra productos de acuerdo a los Pliegos de Condiciones Específicas.

Representante Legal: Persona física o natural acreditada como tal por el Oferente/ Proponente.

Reporte de Lugares Ocupados: Formulario que contiene los precios ofertados en el procedimiento, organizados de menor a mayor.

Resolución de la Adjudicación: Acto Administrativo mediante el cual el Comité de Compras y Contrataciones procede a la Adjudicación al/los oferente(s) del o los Contratos objeto del procedimiento de compra o contratación

Sobre: Paquete que contiene las credenciales del Oferente/Proponente y las Propuestas Técnicas o Económicas.

Unidad Operativa de Compras y Contrataciones (UOCC): Unidad encargada de la parte operativa de los procedimientos de Compras y Contrataciones.

PAFI: Es el Programa de Administración Financiera Integrada del Ministerio de Hacienda, el cual está en proceso interno de pasar a Dirección de Área con una nueva denominación de Dirección de Administración Financiera Integrada (DAFI).

Para la interpretación del presente Pliego de Condiciones Específicas:

- Las palabras o designaciones en singular deben entenderse igualmente al plural y viceversa, cuando la interpretación de los textos escritos lo requiera.
- El término **"por escrito"** significa una comunicación escrita con prueba de recepción.
- Toda indicación a capítulo, numeral, inciso, Circular, Enmienda, formulario o anexo se entiende referida a la expresión correspondiente de este Pliego de Condiciones Específicas, salvo indicación expresa en contrario. Los títulos de capítulos, formularios y anexos son utilizados exclusivamente a efectos indicativos y no afectarán su interpretación.
- Las palabras que se inician en mayúscula y que no se encuentran definidas en este documento se interpretarán de acuerdo a las normas legales dominicanas.
- Toda cláusula imprecisa, ambigua, contradictoria u oscura a criterio de la Entidad Contratante, se interpretará en el sentido más favorable a ésta.
- Las referencias a plazos se entenderán como días calendario, salvo que expresamente se utilice la expresión de "días hábiles", en cuyo caso serán días hábiles de acuerdo con la legislación dominicana.

1.4 Idioma

El idioma oficial de la presente Licitación es el español, por tanto, toda la correspondencia y documentos generados durante el procedimiento que intercambien el Oferente/Proponente y el Comité de Compras y Contrataciones deberán ser presentados en este idioma o, de encontrarse en idioma distinto, deberán contar con la traducción al español realizada por un intérprete judicial debidamente autorizado.

1.5 Precio de la Oferta

Los precios cotizados por el Oferente en el Formulario de Presentación de Oferta Económica deberán ajustarse a los requerimientos que se indican a continuación.

Todas las partidas y/o artículos deberán enumerarse y cotizarse por separado en el Formulario de Presentación de Oferta Económica. Si un formulario de Oferta Económica detalla artículos pero no los cotiza, se asumirá que está incluido en la Oferta. Asimismo, cuando algún artículo no aparezca en el formulario de Oferta Económica se asumirá de igual manera, que está incluido en la Oferta.

El desglose de los componentes de los precios se requiere con el único propósito de facilitar a la Entidad Contratante la comparación de las Ofertas.

El precio cotizado en el formulario de Presentación de la Oferta Económica deberá ser el precio total de la oferta, excluyendo cualquier descuento que se ofrezca.

Los precios cotizados por el Oferente serán fijos durante la ejecución del Contrato y no estarán sujetos a ninguna variación por ningún motivo, salvo lo establecido en los **Datos de la Licitación (DDL).**

1.6 Moneda de la Oferta

El precio en la Oferta deberá estar expresado en moneda nacional, (Pesos Dominicanos, RD$), a excepción de los Contratos de suministros desde el exterior, en los que podrá expresarse en la moneda del país de origen de los mismos.

De ser así, el importe de la oferta se calculará sobre la base del tipo de cambio vendedor del BANCO CENTRAL DE LA REPÚBLICA DOMINICANA vigente al cierre del día anterior a la fecha de recepción de ofertas.

1.7 Normativa Aplicable

El proceso de Licitación, el Contrato y su posterior ejecución se regirán por la Constitución de la República Dominicana, Ley No. 340-06 sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, de fecha dieciocho (18) de agosto del 2006, su modificatoria contenida en la Ley No. 449-06 de fecha seis (06) de diciembre del 2006; y su Reglamento de Aplicación emitido mediante el Decreto No. 543-12, de fecha Seis (06) de septiembre del 2012, por las normas que se dicten en el marco de la misma, así como por el presente Pliego de Condiciones y por el Contrato a intervenir.

Todos los documentos que integran el Contrato serán considerados como recíprocamente explicativos.

Para la aplicación de la norma, su interpretación o resolución de conflictos o controversias, se seguirá el siguiente orden de prelación:

1) La Constitución de la República Dominicana;
2) La Ley No. 340-06, sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones, de fecha 18 de agosto del 2006 y su modificatoria contenida en la Ley No. 449-06 de fecha seis (06) de diciembre del 2006;
3) El Reglamento de Aplicación de la Ley No. 340-06, emitido mediante el Decreto No. 543-12, de fecha Seis (06) de septiembre del 2012;

4) Decreto No. 164-13 para fomentar la producción nacional y el fortalecimiento competitivo de las MIPYMES de fecha diez (10) de junio del 2013.
5) Resolución No. 33-16, de fecha veintiséis (26) de abril del 2016 sobre fraccionamiento, actividad comercial del registro de proveedores y rubro emitida por la Dirección de Contrataciones Públicas.
6) Resolución 154-16, de fecha veinticinco (25) de mayo del 2016 sobre las consultas en línea emitida por el Ministerio de Hacienda.
7) Las políticas emitidas por el Órgano Rector.
8) El Pliego de Condiciones Específicas;
9) La Oferta y las muestras que se hubieren acompañado;
10) La Adjudicación;
11) El Contrato;
12) La Orden de Compra.

1.8 Competencia Judicial

Todo litigio, controversia o reclamación resultante de este documento y/o el o los Contratos a intervenir, sus incumplimientos, interpretaciones, resoluciones o nulidades serán sometidos al Tribunal Superior Administrativo conforme al procedimiento establecido en la Ley que instituye el Tribunal Superior Administrativo.

1.9 Proceso Arbitral

De común acuerdo entre las partes, podrán acogerse al procedimiento de Arbitraje Comercial de la República Dominicana, de conformidad con las disposiciones de la Ley No. 479-08, de fecha treinta (30) de diciembre del dos mil ocho (2008).

1.10 De la Publicidad

La convocatoria a presentar Ofertas en las Licitaciones Públicas deberá efectuarse mediante la publicación, al menos en **dos (02) diarios** de circulación nacional por el término de **dos (2) días consecutivos**, con un mínimo de **quince (15) días hábiles** de anticipación a la fecha fijada para la apertura, computados a partir del día siguiente a la última publicación.

La comprobación de que en un llamado a Licitación se hubieran omitido los requisitos de publicidad, dará lugar a la cancelación inmediata del procedimiento por parte de la autoridad de aplicación en cualquier estado de trámite en que se encuentre.

1.11 Etapas de la Licitación

Las Licitaciones podrán ser de Etapa Única o de Etapas Múltiples.

Etapa Única:
Cuando la comparación de las Ofertas y de la calidad de los Oferentes se realiza en un mismo acto.

Etapa Múltiple:
Cuando la Ofertas Técnicas y las Ofertas Económicas se evalúan en etapas separadas:

Etapa I: Se inicia con el proceso de entrega de los **"Sobres A",** contentivos de las Ofertas Técnicas, acompañadas de las muestras, si procede, en acto público y en presencia de Notario Público. Concluye con la valoración de las Ofertas Técnicas y la Resolución emitida por el Comité de Compras y Contrataciones sobre los resultados del Proceso de Homologación.

Etapa II: Se inicia con la apertura y lectura en acto público y en presencia de Notario Público de las Ofertas Económicas "Sobre B", que se mantenían en custodia y que resultaron habilitados en la primera etapa del procedimiento, y concluye con la Resolución de Adjudicación a los Oferentes/Proponentes.

1.12 Órgano de Contratación

El órgano administrativo competente para la contratación de los bienes a ser adquiridos es la Entidad Contratante en la persona de la Máxima Autoridad Ejecutiva de la institución.

1.13 Atribuciones

Son atribuciones de la Entidad Contratante, sin carácter limitativo, las siguientes:

a) Definir la Unidad Administrativa que tendrá la responsabilidad técnica de la gestión.
b) Nombrar a los Peritos.
c) Determinar funciones y responsabilidades por unidad partícipe y por funcionario vinculado al proceso.
d) Cancelar, declarar desierta o nula, total o parcialmente la Licitación, por las causas que considere pertinentes. En consecuencia, podrá efectuar otras Licitaciones en los términos y condiciones que determine.

1.14 Órgano Responsable del Proceso

El Órgano responsable del proceso de Licitación es el Comité de Compras y Contrataciones. El Comité de Compras y Contrataciones está integrado por cinco (05) miembros:

- El funcionario de mayor jerarquía de la institución, o quien este designe, quien lo presidirá;
- El Director Administrativo Financiero de la entidad, o su delegado;
- El Consultor Jurídico de la entidad, quien actuará en calidad de Asesor Legal;
- El Responsable del Área de Planificación y Desarrollo o su equivalente;
- El Responsable de la Oficina de Libre Acceso a la Información.

1.15 Exención de Responsabilidades

El Comité de Compras y Contrataciones no estará obligado a declarar habilitado y/o Adjudicatario a ningún Oferente/Proponente que haya presentado sus Credenciales y/u Ofertas, si las mismas no demuestran que cumplen con los requisitos establecidos en el presente Pliego de Condiciones Específicas.

1.16 Prácticas Corruptas o Fraudulentas

Las prácticas corruptas o fraudulentas comprendidas en el Código Penal o en la Convención Interamericana contra la Corrupción, o cualquier acuerdo entre proponentes o con terceros, que establecieren prácticas restrictivas a la libre competencia, serán causales determinantes del rechazo de la propuesta en cualquier estado del procedimiento de selección, o de la rescisión del Contrato, si éste ya se hubiere celebrado. A los efectos anteriores se entenderá por:

a) **"Práctica Corrupta",** al ofrecimiento, suministro, aceptación o solicitud de cualquier cosa de valor con el fin de influir en la actuación de un funcionario público u obtener una ventaja indebida con respecto al proceso de contratación o a la ejecución del Contrato, y,

b) **"Práctica Fraudulenta",** es cualquier acto u omisión incluyendo una tergiversación de los hechos con el fin de influir en un proceso de contratación o en la ejecución de un Contrato de obra pública en perjuicio del contratante; la expresión comprende las prácticas colusorias entre los licitantes (con anterioridad o posterioridad a la presentación de las ofertas) con el fin de establecer precios de oferta a niveles artificiales y no competitivos y privar al contratante de las ventajas de la competencia libre y abierta, coercitivas y obstructiva.

1.17 De los Oferentes/ Proponentes Hábiles e Inhábiles

Toda persona natural o jurídica, nacional o extranjera que haya adquirido el Pliego de Condiciones, tendrá derecho a participar en la presente Licitación, siempre y cuando reúna las condiciones exigidas y no se encuentre afectada por el régimen de prohibiciones establecido en el presente Pliego de Condiciones.

1.18 Prohibición a 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 Sub-contralor; 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 incluidas bajo el ámbito de aplicación de la Ley No. 340-06;

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

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

4) Todo personal de la entidad contratante;

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 que 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 suministraren informaciones falsas o que participen en actividades ilegales o fraudulentas relacionadas con la contratación;

12) Las personas naturales o jurídicas que se encuentren 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 I: Para los funcionarios contemplados en los Numerales 1 y 2, la prohibición se extenderá hasta **seis (6) 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 servicio.

En adición a las disposiciones del Artículo 14 de la Ley No. 340-06 con sus modificaciones NO podrán contratar con el Estado dominicano los proveedores que no hayan actualizado sus datos en el Registro de Proveedores del Estado.

1.19 Demostración de Capacidad para Contratar

Los Oferentes/Proponentes deben demostrar que:

1) Poseen las calificaciones profesionales y técnicas que aseguren su competencia, los recursos financieros, el equipo y demás medios físicos, la fiabilidad, la experiencia y el personal necesario para ejecutar el contrato.
2) No están embargados, en estado de quiebra o en proceso de liquidación; sus negocios no han sido puestos bajo administración judicial, y sus actividades comerciales no han sido suspendidas ni se ha iniciado procedimiento judicial en su contra por cualquiera de los motivos precedentes;

3) Han cumplido con sus obligaciones tributarias y de seguridad social;

4) Han cumplido con las demás condiciones de participación, establecidas de antemano en los avisos y el presente Pliego de Condiciones;

5) Se encuentran legalmente domiciliados y establecidos en el país, cuando se trate de licitaciones públicas nacionales;

6) Que los fines sociales sean compatibles con el objeto contractual;

1.20 Representante Legal

Todos los documentos que presente el Oferente/Proponente dentro de la presente Licitación deberán estar firmados por él, o su Representante Legal, debidamente facultado al efecto.

1.21 Subsanaciones

A los fines de la presente Licitación se considera que una Oferta se ajusta sustancialmente a los Pliegos de Condiciones, cuando concuerda con todos los términos y especificaciones de dichos documentos, sin desviaciones, reservas, omisiones o errores significativos. La ausencia de requisitos relativos a las credenciales de los oferentes es siempre subsanable.

La determinación de la Entidad Contratante de que una Oferta se ajusta sustancialmente a los documentos de la Licitación se basará en el contenido de la propia Oferta, sin que tenga que recurrir a pruebas externas.

Siempre que se trate de errores u omisiones de naturaleza subsanable entendiendo por éstos, generalmente, aquellas cuestiones que no afecten el principio de que las Ofertas deben ajustarse sustancialmente a los Pliegos de Condiciones, la Entidad Contratante podrá solicitar que, en un plazo breve, El Oferente/Proponente suministre la información faltante.

Cuando proceda la posibilidad de subsanar errores u omisiones se interpretará en todos los casos bajo el entendido de que la Entidad Contratante tenga la posibilidad de contar con la mayor cantidad de ofertas validas posibles y de evitar que, por cuestiones formales intrascendentes, se vea privada de optar por ofertas serias y convenientes desde el punto de vista del precio y la calidad.

No se podrá considerar error u omisión subsanable, cualquier corrección que altere la sustancia de una oferta para que se la mejore.

La Entidad Contratante rechazará toda Oferta que no se ajuste sustancialmente al Pliego de Condiciones Específica. No se admitirán correcciones posteriores que permitan que cualquier Oferta, que inicialmente no se ajustaba a dicho Pliego, posteriormente se ajuste al mismo.

1.22 Rectificaciones Aritméticas

Para fines de subsanaciones, los errores aritméticos serán corregidos de la siguiente manera:

a) Si existiere una discrepancia entre una cantidad parcial y la cantidad total obtenida multiplicando las cantidades parciales, prevalecerá la cantidad parcial y el total será corregido.

b) Si la discrepancia resulta de un error de suma o resta, se procederá de igual manera; esto es, prevaleciendo las cantidades parciales y corrigiendo los totales.

c) Si existiere una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras.

Si el Oferente no acepta la corrección de los errores, su Oferta será rechazada.

1.23 Garantías

Los importes correspondientes a las garantías deberán hacerse en la misma moneda utilizada para la presentación de la Oferta. Cualquier garantía presentada en una moneda diferente a la presentada en la Oferta será descalificada sin más trámite.

Los Oferentes/Proponentes deberán presentar las siguientes garantías:

1.23.1 Garantía de la Seriedad de la Oferta

Correspondiente al uno por ciento (1%) del monto total de la Oferta.

PÁRRAFO I. La Garantía de Seriedad de la Oferta será de cumplimiento obligatorio y vendrá incluida dentro de la Oferta Económica. La omisión en la presentación de la Oferta de la Garantía de Seriedad de Oferta o cuando la misma fuera insuficiente, conllevará la desestimación de la Oferta sin más trámite.

1.23.2 Garantía de Fiel Cumplimiento de Contrato

Los Adjudicatarios cuyos Contratos excedan el equivalente en Pesos Dominicanos de **Diez Mil Dólares de los Estados Unidos de Norteamérica con 00/100 (US$10.000,00)**, están obligados a constituir una Garantía Bancaria o Pólizas de Fianzas de compañías aseguradoras de reconocida solvencia en la República Dominicana, con las condiciones de ser incondicionales, 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 disposición de la Entidad Contratante, cualquiera que haya sido el procedimiento y la forma de Adjudicación del Contrato. 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.

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.

Cuando hubiese negativa a constituir la Garantía de Fiel Cumplimiento de Contrato, la Entidad Contratante, 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 Reporte de Lugares Ocupados. El nuevo Oferente Adjudicatario depositará la Garantía y suscribirá el Contrato de acuerdo al plazo que le será otorgado por la Entidad Contratante**,** mediante comunicación formal.

1.24 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 de Contrato: Una vez cumplido el contrato a satisfacción de la Entidad Contratante, cuando no quede pendiente la aplicación de multa o penalidad alguna.

1.25 Consultas

Los interesados podrán solicitar a la Entidad Contratante aclaraciones acerca del Pliego de Condiciones Específicas, hasta la fecha que coincida con el **CINCUENTA POR CIENTO (50%)** del

plazo para la presentación de las Ofertas. Las consultas las formularán los Oferentes por escrito, sus representantes legales, o quien éstos identifiquen para el efecto. La Unidad Operativa de Compras y Contrataciones, dentro del plazo previsto, se encargará de obtener las respuestas conforme a la naturaleza de la misma.

Las Consultas se remitirán al Comité de Compras y Contrataciones, dirigidas a:

COMITÉ DE COMPRAS Y CONTRATACIONES
MINISTERIO DE HACIENDA
Referencia: **MH-CCC-LPN- 2017-0010**
Dirección: **Av. México, No.45, Gazcue**
Teléfonos: **809-687-5131, Ext: 2106 2436**
Correo electrónico: **yefernandez@hacienda.gov.do**

1.26 Circulares

El Comité de Compras y Contrataciones podrá emitir Circulares de oficio o para dar respuesta a las Consultas planteadas por los Oferentes/Proponentes con relación al contenido del presente Pliego de Condiciones, formularios, otras Circulares o anexos. Las Circulares se harán de conocimiento de todos los Oferentes/Proponentes. Dichas circulares deberán ser emitidas solo con las preguntas y las respuestas, sin identificar quien consultó, en un plazo no más allá de la fecha que signifique el **SETENTA Y CINCO POR CIENTO (75%)** del plazo previsto para la presentación de las Ofertas y deberán ser notificadas a todos los Oferentes que hayan adquirido el Pliego de Condiciones Específicas y publicadas en el portal institucional y en el administrado por el Órgano Rector.

1.27 Enmiendas

De considerarlo necesario, por iniciativa propia o como consecuencia de una Consulta, el Comité de Compras y Contrataciones podrá modificar, mediante Enmiendas, el Pliego de Condiciones Específicas, formularios, otras Enmiendas o 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 del presente Pliego de Condiciones y en consecuencia, serán de cumplimiento obligatorio para todos los Oferentes/Proponentes.

1.28 Reclamos, Impugnaciones y Controversias

En los casos en que los Oferentes/Proponentes no estén conformes con la Resolución de Adjudicación, tendrán derecho a recurrir dicha Adjudicación. El recurso contra el acto de Adjudicación deberá formalizarse por escrito y seguirá los siguientes pasos:

1. El recurrente presentará la impugnación ante la Entidad Contratante en un plazo no mayor de diez días (10) a partir de la fecha del hecho impugnado o de la fecha en que razonablemente el recurrente debió haber conocido el hecho. La Entidad pondrá a

disposición del recurrente los documentos relevantes correspondientes a la actuación en cuestión, con la excepción de aquellas informaciones declaradas como confidenciales por otros Oferentes o Adjudicatarios, salvo que medie su consentimiento.

2. En los casos de impugnación de Adjudicaciones, para fundamentar el recurso, el mismo se regirá por las reglas de impugnación establecidas en los Pliegos de Condiciones Específicas.

3. Cada una de las partes deberá acompañar sus escritos de los documentos que hará valer en apoyo de sus pretensiones. Toda entidad que conozca de un recurso deberá analizar toda la documentación depositada o producida por la Entidad Contratante.

4. La entidad notificará la interposición del recurso a los terceros involucrados, dentro de un plazo de **dos (2) días hábiles**.

5. Los terceros estarán obligados a contestar sobre el recurso dentro de **cinco (5) días calendario**, a partir de la recepción de notificación del recurso, de lo contrario quedarán excluidos de los debates.

6. La entidad estará obligada a resolver el conflicto, mediante resolución motivada, en un plazo no mayor de **quince (15) días calendario**, a partir de la contestación del recurso o del vencimiento del plazo para hacerlo.

7. El Órgano Rector podrá tomar medidas precautorias oportunas, mientras se encuentre pendiente la resolución de una impugnación para preservar la oportunidad de corregir un incumplimiento potencial de esta ley y sus reglamentos, incluyendo la suspensión de la adjudicación o la ejecución de un Contrato que ya ha sido Adjudicado.

8. Las resoluciones que dicten las Entidades Contratantes podrán ser apeladas, cumpliendo el mismo procedimiento y con los mismos plazos, ante el Órgano Rector, dando por concluida la vía administrativa.

Párrafo I.- En caso de que un Oferente/Proponente iniciare un procedimiento de apelación, la Entidad Contratante deberá poner a disposición del Órgano Rector copia fiel del expediente completo.

Párrafo II.- La presentación de una impugnación de parte de un Oferente o Proveedor, no perjudicará la participación de éste en Licitaciones en curso o futuras, siempre que la misma no esté basada en hechos falsos.

Las controversias no resueltas por los procedimientos indicados en el artículo anterior serán sometidas al Tribunal Superior Administrativo, o por decisión de las partes, a arbitraje.

La información suministrada al Organismo Contratante en el proceso de Licitación, o en el proceso de impugnación de la Resolución Administrativa, que sea declarada como confidencial por el Oferente, no podrá ser divulgada si dicha información pudiese perjudicar los intereses comerciales legítimos de quien la aporte o pudiese perjudicar la competencia leal entre los Proveedores.

1.29 Comisión de Veeduría

Las Veedurías son el mecanismo de control social, que de manera más concreta, acerca a la comunidad al ejercicio y desempeño de la gestión pública y la función administrativa.

Sección II
Datos de la Licitación (DDL)

2.1 Objeto de la Licitación

Constituye el objeto de la presente convocatoria la **"Contratación de empresas para actualización y adecuación del Centro de Datos, donde se albergará el sistema para el control de las operaciones de los establecimientos de juegos y apuestas de la Dirección de Casinos y Juegos de Azar del Ministerio de Hacienda, 2da Convocatoria",** de acuerdo con las condiciones fijadas en el presente Pliego de Condiciones Específicas.

2.2 Procedimiento de Selección

Licitación Pública Nacional de Etapa Única.

2.3 Fuente de Recursos

El MINISTERIO DE HACIENDA, de conformidad con el Artículo 32 del Reglamento No. 543-12 sobre Compras y Contrataciones Públicas de Bienes, Servicios y Obras, ha tomado las medidas previsoras necesarias a los fines de garantizar la apropiación de fondos correspondiente, dentro de los Presupuestos de los años 2017, 2018 y 2019, que sustentarán el pago de todos los bienes adjudicados y adquiridos mediante la presente Licitación. Las partidas de fondos para liquidar las entregas programadas serán debidamente especializadas para tales fines, a efecto de que las condiciones contractuales no sufran ningún tipo de variación durante el tiempo de ejecución del mismo.

2.4 Condiciones de Pago

La Entidad Contratante establece la modalidad de pago por concepto de año para el presente procedimiento, bajo el siguiente esquema:

Primer año correspondiente a los equipos y licencias, así como el soporte y mantenimiento, desglosado de la siguiente manera:

(i) **Anticipo:** El veinte por ciento (20%) del precio del Contrato, se pagará dentro de los treinta (30) días siguientes a la entrega de la garantía de buen del anticipo;*

(ii) **Al entregar las órdenes de compras a fábrica:** El cuarenta por ciento (40%) del precio del Contrato, se pagará dentro de los treinta (30) días siguientes de que el proveedor entregue las órdenes de compras colocadas en fábrica;

(ii) **Al entregar los equipos:** El veinte por ciento (20%) del precio del Contrato, se pagará dentro de los treinta (30) días siguientes de recibidos los bienes y servicios conexos;

(iii) **Puesta en marcha o funcionamiento de los bienes:** El veinte por ciento (20%) del precio del Contrato, se pagará dentro de los treinta (30) días siguientes de la puesta en marcha y funcionamiento de los bienes a satisfacción de la Entidad Contratante.

Segundo año se pagará el cien por ciento (100%), dentro de los treinta (30) días siguientes de cumplirse el inicio del Segundo Año, por concepto de soportes y mantenimientos.

Tercer año correspondiente al cien por ciento (100%), se pagará dentro de los treinta (30) días siguientes de cumplirse el inicio del Tercer Año, por concepto de soportes y mantenimientos.

*La garantía de buen uso de anticipo deberá ser constituida por el equivalente al monto que reciba el adjudicatario, conforme a lo establecido en el artículo 112 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, Reglamento de Aplicación de la Ley No. 340-06 y sus modificaciones.

2.5 Cronograma de la Licitación[3]

ACTIVIDADES	PERÍODO DE EJECUCIÓN
1. Publicación llamado a participar en la licitación	Dos días consecutivos/ dos diarios de circulación nacional. **Miércoles 15 de septiembre del año 2017**
2. Período para realizar consultas por parte de los interesados	50% del plazo para presentar Ofertas Hasta el **Viernes 24 de noviembre del año 2017**
3. Plazo para emitir respuesta por parte del Comité de Compras y Contrataciones	No más allá de la fecha que signifique el 75% del plazo para presentar Ofertas Hasta **Jueves 30 de noviembre del año 2017**
4. Recepción de Propuestas: "Sobre A" y "Sobre B" y apertura de "Sobre A" Propuestas Técnicas y "Sobre B" Propuestas Económicas.	30 días hábiles contados a partir de la última publicación **Miércoles 06 de diciembre del año 2017** **Desde las 8:00AM hasta las 09:30AM.** **Lugar de Recepción: Dirección Jurídica** **Apertura: Sobre "A" 10:00 AM.** **Lugar de Apertura: Salón Matías Ramón Mella, Ministerio de Hacienda, Gazcue, Distrito Nacional.**

[3] **Nota:** Incluir en el cronograma una actividad de reunión técnica o aclaratoria, si procede.

5. Verificación, Validación y Evaluación contenido de las Propuestas Técnicas "Sobre A" y Homologación de Muestras, si procede.	Plazo razonable conforme al objeto de la contratación **Jueves 07 de diciembre del año 2017**
6. Notificación de errores u omisiones de naturaleza subsanables.	Plazo razonable conforme al objeto de la contratación **Jueves 07 de diciembre del año 2017**
7. Periodo de subsanación de ofertas	Plazo razonable conforme al objeto de la Contratación **Vienes 08 de diciembre del año 2017**
8. Período de Ponderación de Subsanaciones	Plazo razonable conforme al objeto de la contratación **Lunes 11 de diciembre del año 2017**
9. Adjudicación	Concluido el proceso de evaluación **Martes 12 de diciembre del año 2017**
10. Notificación y Publicación de Adjudicación	5 días hábiles a partir del Acto Administrativo de Adjudicación **Martes 12 de diciembre del año 2017**
11. Plazo para la constitución de la Garantía Bancaria de Fiel Cumplimiento de Contrato	Dentro de los siguientes 05 días hábiles, contados a partir de la Notificación de Adjudicación **Miércoles 13 de diciembre del año 2017**
12. Suscripción del Contrato	No mayor a 20 días hábiles contados a partir de la Notificación de Adjudicación **Jueves 14 de diciembre del año 2017**
13. Publicación de los Contratos en el portal institución y en el portal administrado por el Órgano Rector.	Inmediatamente después de suscritos por las partes

2.6 Disponibilidad y Adquisición del Pliego de Condiciones

El Pliego de Condiciones estará disponible para quien lo solicite, en la sede central del **MINISTERIO DE HACIENDA,** ubicada en la **Av., México, No. 45, Gazcue** en el horario de **9:00 a.m. / 3:00 p.m., de lunes a viernes**, en la fecha indicada en el Cronograma de la Licitación y en la página Web de la institución **www.hacienda.gob.do** y en el portal administrado por el Órgano Rector**,** www.comprasdominicana.gov.do, para todos los interesados.

El Oferente que adquiera el Pliego de Condiciones a través de la página Web de la institución, **www.hacienda.gob.do** o del portal administrado por el Órgano Rector, www.comprasdominicana.gov.do, deberá enviar un correo electrónico a **yefernandez@hacienda.gov.do**, o en su defecto, notificar al **Comité de Compras y Contrataciones del Ministerio de Hacienda** sobre la adquisición del mismo, a los fines de que la Entidad Contratante tome conocimiento de su interés en participar.

2.7 Conocimiento y Aceptación del Pliego de Condiciones

El sólo hecho de un Oferente/Proponente participar en la Licitación implica pleno conocimiento, aceptación y sometimiento por él, por sus miembros, ejecutivos y su Representante Legal, a los procedimientos, condiciones, estipulaciones y normativas, sin excepción alguna, establecidos en el presente Pliego de Condiciones, el cual tienen carácter jurídicamente obligatorio y vinculante.

2.8 Descripción de los Bienes

2.8.1 Descripción de los Bienes

2.8.1.1 Sistemas de Seguridad Lógica

Ministerio de Hacienda			
Especificaciones Técnicas para la Contratación de empresas para actualización y adecuación del Centro de Datos, donde se albergará el sistema para el control de las operaciones de los establecimientos de juegos y apuestas de la Dirección de Casinos y Juegos de Azar del Ministerio de Hacienda			
No. De Partida	**Cantidad**	***Descripción***	**Especificaciones Técnicas**
		Sistemas de Seguridad Lógica	***Sistemas de Seguridad Lógica integrada para el Ministerio de Hacienda y dependencias***
A.0100		***Condiciones Generales a ser ofertadas y cumplidas para todas las soluciones ofertadas:***	
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 en este lote 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 de alta disponibilidad***	Todas las soluciones ofertadas en este lote deben incluir y describir explícitamente configuraciones con redundancia de alta disponibilidad en las mismas. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra.
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.
A.05		***Gerente de Proyecto***	Debe incluirse y describirse explícitamente la asignación de un gerente de proyectos dedicado certificado PMP 100% de su tiempo a la implantación de todas las soluciones ofertadas en este lote durante todo el tiempo que sea necesario y requerido por el Ministerio de Hacienda. Se debe incluir en la propuesta el currículo de este gerente de proyectos propuesto.
A.06		***Project Plan***	Debe incluirse y describirse explícitamente el Project Plant en formato de MS Project para la implantación de todas las soluciones ofertadas en este lote, así como los currículos del personal que sería asignado al mismo. El oferente que resulte ganador deberá mantener y actualizar este Project Plan con periodicidad semanal, y deberá justificar por escrito cualquier cambio que ocurriese con respecto al original.
A.07		***Dimensionamiento General***	Para los fines de dimensionamiento general pertinentes a cada solución propuesta, en caso de ser necesario, se deben licenciar 1400 usuarios locales, 1400 dispositivos, 500 Gbps de Tráfico de Internet y 400 máquinas de servidores virtuales para ambientes de aplicaciones. Este dimensionamiento tiene precedencia sobre cualquier error y/u omisión de las especificaciones de cada solución si se diese esa situación. Otros tipos de dimensionamientos particulares a cada solución se especifican en cada una de las mismas.

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 3 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. 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 ofrecerse en la Ciudad de Santo Domingo y deben incluir toda la documentación y material de soporte de los mismos. En caso de no poder ser ofrecidos en la Ciudad de Santo Domingo, se deben incluir los costos de viáticos para los mismos.
3.1000	1400	***Solución Integrada de Endpoint Security, Anti-Virus, Anti-malware, Anti-spyware y Data Loss Prevention***	Se debe proveer una solución integrada de Endpoint Security para los 1400 dispositivos de la entidad.
3.1001			La solución deberá soportar los siguientes sistemas operativos de servidores:
3.1002			Windows Server 2012, 2012 R2, and 2012 R2 Update 1: Essentials, Standard, Datacenter (incluyendo Server Core mode)
3.1003			Windows Storage Server 2012 and 2012 R2
3.1004			Windows Server 2008 and 2008 R2: Standard, Datacenter, Enterprise, Web (incluyendo Server Core mode)
3.1005			Windows Storage Server 2008 and 2008 R2
3.1006			Windows Small Business Server 2011
3.1007			Windows Small Business Server 2008
3.1008			Windows Embedded Standard 2009
3.1009			Windows Point of Service Ready 2009
3.1010			Windows Point of Service 1.1
3.1011			La solución deberá soportar los siguientes sistemas operativos de clientes:
3.1012			Windows 10 Anniversary Update

3.1013			Windows 10 November Update
3.1014			Windows 10
3.1015			Windows 8.1 Update 1
3.1016			Windows 8 (no incluyendo Windows RT edition)
3.1017			Windows 7
3.1018			Windows To Go (All versions)
3.1019			Windows Vista
3.1020			Windows Embedded 8: Pro, Standard, Industry
3.1021			Windows Embedded Standard 7
3.1022			Windows Embedded for Point of Service (WEPOS)
3.1023			MAC Sierra 10.12
3.1024			MAC El Capitán 10.11
3.1025			MAC Yosemite 10.10
3.1026			MAC Mavericks 10.9
3.1027			La solución debe ser administrada de forma centralizada.
3.1028			La solución debe poder ser administrada de manera local o desde la nube.
3.1029			Microsoft Internet Explorer (versiones 7, 8, 9, 10, and 11)
3.1030			Mozilla Firefox (versiones desde 3.0 a 35)
3.1031			Google Chrome (versiones desde 4.0 a 49)
3.1032			Se debe poder desplegar la solución mediante un agente.
3.1033			La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.
3.1034			La solución debe avisar sobre los posibles conflictos que existan de la solución a otras soluciones de anti-virus y firewall instalados previamente en la máquina.
3.1035			Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.
3.1036			La solución debe poder desplegar una aplicación cliente standalone que pueda gestionar cambios localmente en caso de que se necesite.

3.1037			Se debe poder restringir completamente o parcialmente al acceso a la consola cliente para configurar parámetros individuales sobre el host.
3.1038			La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador.
3.1039			Puede existir más de una configuración de idioma para la aplicación cliente.
3.1040			La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de Prevención de Amenazas, control web, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.
3.1041			La solución debe permitir la integración a esta plataforma colaborativa, de un módulo de intercambio de reputación LOCAL, basada en la información recolectada por las diferentes soluciones de seguridad en el ambiente de la empresa. Esto es adicional y no debe confundirse con las fuentes de inteligencia global.
3.1042			La solución debe poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente.
3.1043			Se debe poder configurar acciones sobre infecciones identificadas:
3.1044			Denegar acceso
3.1045			Limpiar
3.1046			Eliminar
3.1047			Ninguna
3.1048			La solución debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí.
3.1049			Se deben reportar eventos de amenazas directamente sobre la consola cliente y visibles desde la consola de administración de la solución.
3.1050			La solución debe poder habilitar la opción de escaneo de click-derecho sobre carpetas específicas.

3.1051			Es requerido que la solución soporte archivos DAT V2 y V3 de detección de amenazas.
3.1052			Debe contar con mecanismos de protección de exploits Generic Buffer Overflow Overflow Protection (GBOP) o integración con Microsoft DEP (Data Execution Prevention).
3.1053			La solución debe contar con características de protección Kevlar para navegadores web (Active X).
3.1054			La solución debe poder integrarse con tecnología SEMP (Intel Supervisor Mode Execution Protection) en sistemas operativos Windows 8.
3.1055			La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de IE, sean JavaScript o VBScript.
3.1056			La solución debe poder configurar mediante reglas o políticas de protección de:
3.1057			Entradas y llaves de registro de Windows.
3.1058			Prevención de creación de ejecutables portables (.INI, .PIF).
3.1059			Creación de archivos autorun.
3.1060			Prevención de uso de archivos TFTP (Trivial File Transfer Protocol).
3.1061			Contra lectura de archivos en cache de IE.
3.1062			Creación y modificación remota de archivos o carpetas.
3.1063			Acceso remoto de archivos o carpetas.
3.1064			.EXE, .BAT y otros ejecutables bajo la llave de registro HKEY_CLASSES_ROOT.
3.1065			Modificación de procesos core de Windows.
3.1066			Modificación de configuraciones de exploradores y navegadores web.
3.1067			Proteger procesos con sub reglas personalizadas
3.1068			Asignar las reglas por nombre de usuario
3.1069			La solución debe permitir la implementación de un módulo de contención de aplicaciones basado en la reputación de dicha aplicación obtenida a través del módulo de reputación Local. Las aplicaciones que se ejecuten en modo contenido no podrán realizar acciones específicas definidas desde la consola de administración.
3.1070			La solución de antivirus debe ser además compatible con sistemas Linux CentOS, Red Hat, SuSe y Ubuntu

3.1071			Las políticas de antivirus definidas desde la consola deben poder ser aplicables para cualquier sistema operativo soportado. No se aceptará tener que definir políticas diferentes para diferentes sistemas operativos
3.1072			El modulo debe permitir/bloquear tráfico de red para protocolos no soportados.
3.1073			Permitir o bloquear trafico solo hasta que el modulo y servicios de firewall este arriba.
3.1074			Habilitar/deshabilitar protección IP Spoof
3.1075			Habilitar/deshabilitar alertas de intrusión de Firewall
3.1076			Agregar dominios específicos para bloqueo DNS.
3.1077			La solución debe poder recopilar log en eventos lanzados directamente sobre el cliente y reportar incidentes en la consola de administración central.
3.1078			Cada una de las reglas debe ser aplicable para tráfico entrante como para tráfico saliente del cliente.
3.1079			Las reglas de trafico deben ser soportadas para protocolos IP:
3.1080			Ipv4
3.1081			Ipv6
3.1082			La solución debe aplicar reglas de tráfico para conexiones:
3.1083			Alámbricas
3.1084			Inalámbricas
3.1085			Virtuales
3.1086			Las reglas de tráfico deben poder extenderse a ejecutables por medio de la especificación de ruta (se pueden utilizar wildcards).
3.1087			El modulo debe poder incluir reglas en base a los protocolos y puertos más conocidos del mundo.
3.1088			Se debe poder administrar redes y ejecutables de confianza desde la interfaz de usuario de los endpoints.
3.1089			La herramienta debe contar con un mecanismo de conocimiento global de amenazas que permita configurar bloqueo de conexiones de alto riesgo en base a reputación.
3.1090			La solución debe poder bloquear de forma automática sitios con clasificación de riesgo alto que puedan afectar los equipos y/o la red.
3.1091			La solución debe tener la capacidad de bloquear y/o dejara al usuario decidir qué acción tomar en caso que el sitio que se esté visitando por alguna razón no cuente con una clasificación en ese momento.

3.1092			La solución debe contar con un elemento visual que permita identificar el riesgo del sitio visitado en los navegadores soportados.
3.1093			La solución incluso debe tener la capacidad de ayudar a la institución permitiéndole definir reglas de filtrado de URL por categorías.
3.1094			La solución debe tener la capacidad de evitar el acceso a sitios de phishing.
3.1095			La solución deberá poder evitar descargar malware, ayudando así a tener que la protección sea proactiva.
3.1096			La solución deberá de contar con alrededor de 100 categorías de sitios web.
3.1097			La solución debe poder especificar que navegadores sean los únicos autorizados para navegar a internet.
3.1098			La solución debe tener la capacidad de definir rangos de IP privadas (intranet) que no sean analizadas por la herramienta para bloqueo de sitios web.
3.1099			La solución debe tener la capacidad de forzar búsquedas seguras con los buscadores al menos cuatro de los motores de búsqueda más usados (Google, MSN, Yahoo, Terra, UOL, Ask).
3.1100			La solución debe poder bloquear iFrames de HTML o advertir de sitios que contengan.
3.1101			La solución debe tener categorías sincronizadas con una base de datos de reputación global de amenazas.
3.1102			La clasificación deberá ser en tiempo real y contra una base de datos de reputación que al menos correlacione archivos, URL´s, y correos electrónicos todo esto en la nube.
3.1103			La solución debe tener la capacidad de personalizar los mensajes que le aparezcan al usuario cuando una política sea violada.
3.1104			La solución debe tener la capacidad de definir un logotipo para mostrarlo en los mensajes de violación a las políticas.
3.1105			Se deben poder ver reportes de amenazas web detectadas y políticas violadas.
3.1106			La solución debe captar logs o registros para eventuales temas de compliance y troubleshooting.
3.1107			La solución debe estar en la capacidad de identificar cuando se está una solución de proxy y apagarse en la presencia de este.

3.2000	***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 e integración con la solución de Sandboxing***	Los Gateways de Manejo y Control de Seguridad Integrada redundante debe ser capaz de manejar los siguientes aspectos de seguridad:
3.2001			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.
3.2002			Debe ser capaz de soportar, estar configurada y licenciada para un throughput a la velocidad de conexión agregada hacia Internet de mínimo 500 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 60 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+ Debe soportar control de acceso para por lo menos 150 servicios y/o protocolos predefinidos
3.2003			Debe permitir definir reglas de seguridad que puedan ser esforzadas 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.
3.2004			Debe soportar métodos de autenticación basados en clientes, usuarios y sesiones.
3.2005			La comunicación entre los servidores de gerencia y los Gateways de Seguridad deben ser encriptados y autenticados con Certificados PKI

3.2006			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.
3.2007			Deben soportarse los siguientes esquemas de autenticación de usuarios: Tokens (SecureID), TACACS, RADIUS y Certificados Digitales
3.2008			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
3.2009			Debe soportar la configuración de gateways en stacks dobles o con un interfase de unión o como una sub-interfase de un interfase de unión.
3.2010			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
3.2011			Debe soportar seguimiento y logs que muestren el tráfico IPv6. Debe soportar la habilidad de mostrar tablas de ruteo IPv6.
3.2012			La solución debe soportar los siguientes RFCs IPv6:
3.2013			RFC 1981 Path Maximum Transmission Unit Discovery for IPv6
3.2014			RFC 2460 IPv6 Basic specification
3.2015			RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
3.2016			RFC 3596 DNS Extensions to support IPv6
3.2017			RFC 4007 IPv6 Scoped Address Architecture
3.2018			RFC 4193 Unique Local IPv6 Unicast Addresses
3.2019			RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – 6in4 tunnel is supported.
3.2020			RFC 4291 IPv6 Addressing Architecture (which replaced RFC1884)
3.2021			RFC 4443 ICMPv6
3.2022			RFC 4861 Neighbor Discovery
3.2023			RFC 4862 IPv6 Stateless Address Auto-configuration
3.2024			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

3.2025			La solución debe pertenecer al cuadrante de líderes del Cuadrante Mágico de Gartner para las soluciones de Firewall e IPS
3.2026			Las soluciones de IPS y de Firewall deben estar integradas en una única plataforma
3.2027			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.
3.2028			La solución de IPS debe proveer pre configurada por lo menos dos perfiles y/o políticas que puedan ser usadas de forma inmediata
3.2029			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
3.2030			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.
3.2031			Los IPS deben incluir una modalidad de Troubleshooting que permita al perfil en uso que solo detecte sin modificar las protecciones individuales
3.2032			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.
3.2033			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.

3.2034			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
3.2035			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
3.2036			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
3.2037			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.
3.2038			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.
3.2039			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
3.2040			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
3.2041			Debe soportar ambientes de terminal servers. Debe integrarse de forma nativa con servicios de directorios, IF-MAP y RADIUS
3.2042			El impacto de estos servicios debe ser menor al 3% en los controladores de dominio. La solución debe soportar terminales y servidores Citrix

3.2043			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.
3.2044			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
3.2045			La base de datos de la Solución para Control de Aplicaciones y Filtrado de URL debe contener más de 6000 aplicaciones conocidas. Debe tener una categorización de URLs que contenga mas de 200 millones de URLs y que cubra más del 85% del millón de sitios topes de Alexa
3.2046			La solución debe ser capaz de crear reglas de filtrado con múltiples categorías. Debe ser capaz de crear filtros para un único site.
3.2047			Debe tener granularidad de usuarios y grupos para las reglas de seguridad.
3.2048			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
3.2049			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.
3.2050			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
3.2051			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.
3.2052			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.

3.2053			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.
3.2054			La solución debe tener mecanismos configurables de Bypass. Debe proveer un mecanismo de override para la categorización de la base de datos de URLS.
3.2055			El control de las aplicaciones y las políticas de seguridad de los URLF deben reportar el conteo de usos de las reglas
3.2056			La solución debe incluir las aplicaciones de Anti-BOT y Anti-Virus integradas en los Gateways de Seguridad.
3.2057			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.
3.2058			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.
3.2059			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
3.2060			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
3.2061			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.

3.2062			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.
3.2063			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.
3.2064			El Anti-Virus debe soportar mas de 50 motores de Anti-Virus basados en la nube. Debe soportar escaneo de links dentro de los emails y escanear archivos que están pasando mediante el protocolo CIFS
3.2065			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
3.2066			Debe soportar Perfect Forward Secrecy (PFS, ECDHE conjuntos de cifrado), y AES-NI, AES-GCM para mejoras en el flujo
3.2067			Deben incluirse funcionalidades para la emulación de amenazas y sandboxing integradas a la inspección de SSL.
3.2068			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
3.2069			La solución debe ofrecer la funcionalidad de coordinación e integración con soluciones de Emulación de Amenazas (Sandboxing).
3.2070			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
3.2071			La Solución de Seguridad debe ser una arquitectura de prevención de amenazas completa y multinivel con mínimo de funcionalidades de: IPS, AV, AB, URLF, APP FW

3.2072			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
3.2073			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
3.2074			La solución no debe requerir infraestructura separada para protección de email y protección de WEB.
3.2075			Los dispositivos deben soportar instalación en Clusters de alta disponibilidad y deben estar configurados y ofertados en este esquema
3.2076			La solución debe ser capaz de emular archivos almacenados ejecutables, documentos JAVA y FLASH, específicamente:
3.2077			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
3.2078			La solución debe ser capaz de emular ejecutables, archivos almacenados, documentos, JAVA y Flash específicamente dentro de los siguientes protocolos:
3.2079			HTTP,HTTPS,FTP,SMTP,CIFS(SMB), SMTP TLS
3.2080			El motor de emulación debe soportar múltiples sistemas operativos tales como Windows 7,8,10 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
3.2081			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
3.2082			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

3.2083			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.
3.2084			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
3.2085			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.
3.2086			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
3.2087			La solución de emulación de amenazas debe permitir Restricciones Geográficas, las cuales permiten que las emulaciones sean restringidas a Países en específico.
3.2088			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
3.2089			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
3.2090			La Solución debe ser capaz de emular y extraer archivos embebidos en documentos. Debe ser capaz de escanear documentos que contengan URLs
3.2091			La solución debe monitorear las actividades sospechosas en:

3.2092			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.
3.2093			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.
3.2094			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)
3.2095			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
3.2096			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.

3.2097			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
3.2098			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
3.2099			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.
3.2100			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
3.2101			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.
3.2102			Debe soportar SSL VPN clientless para acceso remoto. Deben soportar VPNs L2TP incluyendo los clientes para Iphones.
3.2103			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.
3.2104			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.

3.2105			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
3.2106			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.
3.2107			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.
3.2108			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.
3.2109			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.
3.2110			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.

3.2111			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.
3.2112			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
3.2113			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.
3.2114			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.
3.2115			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.
3.2116			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.

3.2117			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
3.2118			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
3.2119			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.
3.2120			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.
3.2121			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.

3.2122			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
3.2123			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.
3.2124			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.
3.2125			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.
3.2126			La solución debe ser capaz de detectar ataques de Negación 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.

3.2127			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
3.2128			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.
3.2129			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.
3.2130			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.
3.2131			La solución de Seguridad debe incluir una aplicación completamente integrada de Data Loss Prevention (DLT) que debe ser manejada de manera centralizada con las otras aplicaciones de seguridad de esta suite.

3.2132			La aplicación de DLT debe tener mecanismos para el manejo de auto-incidentes de usuarios finales. Debe tener un mínimo de 500 tipos de data predefinidos. Debe poseer un lenguaje de creación de scripts para poder definir tipos de data relevantes a cada organización. Debe alertar al dueño del tipo de data cuando ocurre un incidente. Debe cubrir tipos de transporte SMTP, HTTP/HTTPS y protocolos FTP y TCP
3.2133			La solución integrada de seguridad debe ofrecer una funcionalidad completa para asegurar los dispositivos móviles. Debe soportar tanto los dispositivos gerenciados como los no gerenciados tales como los BYOD.
3.2134			La solución debe incluir todo el hardware, software, y licencias necesarias para poder manejar el siguiente dimensionamiento: Manejo de un Ancho de Banda Agregada de Acceso a Internet de por lo menos 500 Gbps y capacidad de crecimiento para por lo menos 1 Gbps. Capacidad de manejo de mínimo de 8 conexiones independientes a distintos proveedores de servicios. Configurada y licenciada para manejar un mínimo de 1200 end points, 1200 buzones de correo y 400 máquinas virtuales de servidores que pueden correr sistemas operativos Windows, Linux o Solaris
3.2135			La solución debe tener un mínimo de 100 reglas de seguridad pre configuradas
3.2136			La solución integrada debe ofrecer las siguiente soluciones de seguridad para todo este dimensionamiento : Firewall, Prevención de Intrusos, Control de Aplicaciones y Filtrado de URL, Anti Virus, Anti BOT, Emulación de Amenazas y Extracción de Amenazas, VPNs IPsec, Data Loss Prevention
3.2137			Las soluciones de Hardware deben ser ofertadas en clusters de alta disponibilidad con fuentes de poder y abanicos redundantes.
3.2138			La solución debe ser capaz de trabajar de forma coordinada e integrada con la solución de seguridad de Sandboxing
3.3000	1	***Solución de Sandboxing***	La solución deberá 100% compatible con la plataforma de Correo de la Entidad. 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.
3.3001			La solución debe funcionar en equipos propuestos a ser instalados en las premisas de la entidad contratante

3.3002			Deberá permitir la ejecución de código malicioso en sistemas operativos virtuales
3.3003			Deberá contar con mecanismos que permitan la evaluación del malware en sistemas operativos no virtualizados dentro de la solución
3.3004			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.
3.3005			Deberá permitir la detección de modificación de Archivos, comportamiento de procesos, comportamiento de registros, comportamientos de red
3.3006			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
3.3007			Deberá soportar como mínimo los siguientes tipos de Archivos :
3.3008			CAB,PIF,swf,jar,js/jse,pdf ,doc,docx ,dot,dotx
3.3009			,dotm,docm,xlt ,xls ,xlsx ,xlm,xltx ,xlsm ,xltm
3.3010			,xlsb,xla ,xlam ,xll,xlw ,ppt,pptx,pps,pptm ,potx,potm
3.3011			,ppam,ppsx ,ppsm,sldx ,sldm,exe ,com,tar ,zip,rar
3.3012			,Seven-Z,gz,tgz,bz2 ,rtf,scr ,csv,iso,cpl,wsf,wsh,vbs,vba,vbe
3.3013			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.
3.3014			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
3.3015			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)
3.3016			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

3.3017			Deberá permitir que los archivos que son analizados con el OS Sandbox deben entregar un análisis posterior a la ejecución de las siguientes características:
3.3018			Descarga de Virus
3.3019			Modificación de Registro
3.3020			Conexiones externas a Ips maliciosas
3.3021			Infección de procesos
3.3022			El equipo deberá contar como mínimo con 2 TB de capacidad de disco
3.3023			El equipo deberá soportar como mínimo 1300 usuarios y capacidad de emulación de archivos de hasta 200000 por mes
3.3024			El equipo deberá contar como mínimo con 5 Interfaces a 1Gbps RJ45 y opción de adicionar por lo menos 7 más
3.3025			La solución debe permitir la emulación de tamaño de archivos de más de 15 Mb
3.3026			La solución debe ser capaz de detectar ROP y otras técnicas de explotación (por ejemplo escalamiento de privilegios) controlando el flujo de CPU
3.3027			La solución debe tener capacidades anti-evasión detección ejecución caja de arena(sandboxing)
3.3028			El motor de emulación debe tener la capacidad de detección anti-virtual machine
3.3029			Solución debe ser resistente a los casos en que el malware ejecute un reinicio o un apagado de la máquina virtual de Sandboxing
3.3030			La solución debe emular las actividades reales de los usuarios, tales como clics del ratón, pulsaciones de teclas, etc
3.3031			La solución debe eliminar las amenazas y eliminar contenido explotable, incluyendo el contenido activo y objetos incrustados
3.3032			La solución debe ser capaz de reconstruir los archivos con los elementos de seguridad conocidos
3.3033			La solución debe proporcionar capacidad de convertir archivos reconstruidos a formato PDF
3.3034			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.
3.3035			Solución debe ser resistente a los retrasos implementados en el código shell o etapas de malware.

3.3036			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.
3.3037			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.
3.3038			Las soluciones de Hardware deben ser ofertadas en clusters de alta disponibilidad con fuentes de poder y abanicos redundantes.
3.4000	1	***Solución de Seguridad para Database Activity Monitoring (DAM)***	La solución debe ser basada en software permitiendo la mayor escalabilidad posible a nivel de crecimiento futuro.
3.4001			La consola de administración debe permitir virtualizarse y estar en capacidad de procesar el manejo de instancias ilimitadas de bases de datos.
3.4002			La solución deberá tener una arquitectura que no sea intrusiva con la capa de datos de la base de datos como tal.
3.4003			La solución debe permitir el bloqueo y la configuración de cuarentenas, mientras se analiza el incidente presentado.
3.4004			La solución deberá trabajar leyendo memoria compartida, para evitar intrusiones sobre los datos de la base de datos.
3.4005			Los servidores donde se instalen los sensores de monitoreo, no deberán requerir reinicio
3.4006			La solución deberá soportar el monitoreo de clúster de DBMs.
3.4007			La solución deberá contar con la funcionalidad de parcheo virtual, para brindar seguridad al ambiente de bases de datos y conocer el impacto cuando el fabricante de la base de datos no haya liberado el parche aún.
3.4008			La solución deberá incluir un set de reglas predefinidas, enfocadas en la posibilidad de monitorear y/o bloquear, ataques comunes como SQL injection.
3.4009			La solución deberá incluir un módulo de análisis de vulnerabilidades que se base no solamente en carencia de parches, sino debilidades de configuraciones y vulnerabilidades comunes de los motores, según el CVE y sugerencias en resolver la brecha en caso de que exista.

3.4010			La solución deberá contar con un panel de configuración de reglas intuitivo, donde se facilite la asociación de parámetros de sentencias como CMDTYPE, INFLOW, MODULE, OSUSER, etc,.
3.4011			La solución deberá soportar al menos los siguientes motores, a nivel de monitoreo de la actividad de bases de datos: Oracle versión 8.1.7 and later, running on Sun Solaris, IBM AIX, Linux, HP-UX, Microsoft Windows, including Oracle RAC and Oracle Exadata Microsoft SQL 2000 and later on any supported Windows platform IBM DB2 LUW 9.5, and later Sybase ASE 12.5 and later on all supported platforms Teradata 12, 13, 13.10, 14,15, and 15.1 on Linux MySQL 5.1, 5.5, 5.6 and 5.7 on Linux MariaDB versión 5.5 (5.5.32 and later), 10.0 and 10.1 on Linux IBM DB2 for Z/OS with CorreLog IBM DB2 for iSeries (AS/400) with Raz-Lee SAP HANA SPS 09, Revision 91 and later PostgreSQL 9.2 and later on Linux
3.4012			La solución deberá soportar al menos los siguientes motores, a nivel de escaneo de vulnerabilidades: Oracle 8i or later Microsoft SQL Server 2000 or later Microsoft SQL Azure IBM DB2 8.1 or later for Linux, Unix, and Windows MySQL versión 4.0 or later PostgreSQL versión 8.3 or later Sybase ASE versión 12.5 or later SAP HANA v1 and later Teradata v12, v13, v14 — Database discovery, sensitive data discovery, custom checks, and password cracking Informix v10.0, v11.1, v11.5, v11.7 — Database discovery, sensitive data discovery and custom checks
3.4013			La solución deberá permitir la creación de reglas para bloquear un usuario local de la DB que intente realizar conexiones a la DB
3.4014			La solución deberá permitir la creación de reglas para bloquear un usuario del dominio que intente realizar conexiones a la DB
3.4015			La solución deberá permitir la creación de reglas para bloquear conexiones a la DB desde una dirección IP especifica

3.4016			La solución deberá permitir la creación de reglas para bloquear sentencias de escritura a un determinado usuario y solo permitir sentencias de lectura.
3.4017			La solución deberá permitir la creación de reglas para bloquear Sentencias especificas a la DB. Permitir o bloquear el acceso a una determinada tabla.
3.4018			La solución deberá permitir la generación de reportes de la actividad de un usuario especifico
3.4019			La solución deberá permitir la generación de reportes estándar como TOP IP, TOP Usuarios, TOP Sentencias, etc
3.4020			La solución deberá permitir la generación de alertas en la consola y mediante correo electrónico ante un evento en particular o un comportamiento anómalo.
3.4021			La solución deberá permitir hacer un trigger de alerta, cuando un usuario saque un determinado número de registros, de una base de datos.
3.4022			La solución deberá proveer protección contra los ataques de ofuscación avanzados.
3.4023			La solución deberá permitir la creación de reglas de monitoreo de acceso a las bases de datos, por horario o días hábiles.
3.4024			La solución deberá poder monitorear aplicaciones que en un momento dado, estén accediendo la base de datos y crear reglas de alerta cuando aplicaciones no permitidas, estén accediendo la base de datos.
3.4025			La consola deberá permitir una gestión centralizada de los agentes de monitoreo.
3.4026			La solución deberá tener la flexibilidad para no ser intrusivo y solo hacer monitoreo de transacciones a nivel de red.
3.4027			La solución deberá poder integrarse a una solución SIEM.
3.4028			La solución deberá permitir la configuración de notificaciones vía correo, parámetros de SNMP, envío y/o almacenado de logs.
3.4029			La solución deberá permitir la creación de backups de reglas configuradas.
3.4030			La solución deberá ser basada en software, para evitar hacer rediseño de la red de datos.
3.4031			La solución deberá incluir una herramienta de manejo de casos (incident management) embebida.
3.4032			La solución deberá poder hacer el monitoreo de actividad sobre las bases de datos sin requerir que la auditoría del motor de base de datos esté activa.

3.4033			La solución deberá permitir la creación de una línea base (wizard) asociada a parámetros normales de uso y/o regulaciones de compliance como por ejemplo PCI, para enfocar las alertas en las desviaciones de la línea base.
3.4034			La solución deberá permitir el enmascaramiento de datos, usando mecanismos como expresiones regulares, para evitar la visualización de información personal identificable o sensible como números de tarjetas de crédito, que pudieran estar en los campos de las bases de datos.
3.4035			La solución debe permitir la integración con soluciones de directorio como Microsoft AD.
3.4036			La solución debe incluir como mínimo en las alertas, información de timestamp, usuario de sistema operativo, usuario de base de datos, sentencia ejecutada, aplicación, objetos accedidos, CMDTYPE, DBMS y regla que hizo match.
3.4037			La solución debe permitir la generación de reportes de vulnerabilidades diferenciales, asociando valores de riesgo cualitativo (alto, medio y bajo).
3.4038			La solución debe permitir la creación de reportes personalizados.
3.4039			La solución debe permitir la generación de reportes de auditoría DML y archiving de eventos.
3.4040			Dentro de los reportes de auditoría DML, debe existir la posibilidad de generar dichos reportes enriquecidos, con información del result set.
3.4041			La solución debe contar con un módulo de construcción personalizada de queries, con el objetivo de generar reportes personalizados, asociados a dichos queries.
3.5000	1	***Solución de Seguridad SIEM (Security Information and Event Management)***	La solución SIEM a ofertar debe constar de uno o más appliances (hardware) centralizado y/o distribuido e incluir agentes, clientes y componentes necesarios para cumplir los requerimientos técnicos y funcionales.
3.5001			La arquitectura de la solución propuesta deberá ser flexible, por lo tanto puede estar compuesta por appliance endurecido y asegurado por el fabricante y/o por módulos de appliance virtuales, estos también creados y asegurados por el fabricante de la solución. La solución ofertada debe ser de alta disponibilidad y redundante

3.5002			La solución SIEM deberá soportar la recolección de al menos 1500 eps, en un entorno de arquitectura que permita el crecimiento de la solución de forma modular y conforme el proyecto lo requiera. El soporte de EPS debe ser de tráfico sostenido permitiendo además picos que excedan esas capacidades.
3.5003			La solución SIEM deberá ofrecer la capacidad de recolección de hasta 1500 Eventos por Segundo (EPS) y permitir picos de eventos adicionales sin que exista pérdida de eventos. La solución deberá permitir visualizar estadísticos de recolección de EPS, con el objetivo de mantener una correcta línea de funcionalidad.
3.5004			El licenciamiento de la solución SIEM, deberá ser basado en cantidad de EPS y no en la cantidad de dispositivos que se deban integrar.
3.5005			La solución SIEM ofertada debe constar en el ultimo “cuadrante de líderes” del Cuadrante Mágico de Gartner en SIEM (Magic Quadrant for Security Information and Event Management) . El oferente deberá incluir en su oferta dicho reporte, indicando la posición de la marca en el cuadrante.
3.5006			La solución SIEM debe contar de forma integrada y sin necesidad de licenciamiento aparte, un modulo para la creación de nuevos recolectores para tecnologías no soportadas por el fabricante de forma nativa.
3.5007			La solución SIEM deberá contar con un módulo que permita recolectar a manera de sniffer información de sentencias transaccionales a bases de datos con el objetivo de monitorear, analizar, correlacionar y alertar estos eventos. La solución no deberá requerir modificaciones en las configuraciones en las bases de datos a monitorear
3.5008			La solución SIEM deberá permitir entre otros usos monitorear, detectar y tomar medidas correctivas a través de la integración nativa con elementos de seguridad en el endpoint y en el perímetro, al momento de detectar comportamientos asociados a amenazas avanzadas. La solución debe permitir agregar indicadores de compromiso (IOC) los cuales permitan incrementar las capacidad de análisis que posee la herramienta.

3.5009			La solución SIEM deberá estar en capacidad detectar el mal uso de los recursos de navegación generados por los usuarios internos. Este monitoreo debe ser realizado a través de la integración con herramienta de filtro de contenido, para el monitoreo de categorías e indicadores de compromiso para identificar posibles accesos a sitios maliciosos no categorizados.
3.5010			LA solución SIEM debe permitir la creación de paneles y el monitoreo de actividad de usuarios privilegiados en el dominio tales como: Monitoreo del manejo de cuentas (altas, bajas, reset password, etc); elevación de privilegios, monitoreo de cuentas de usuarios VIP, monitoreo de cuentas de usuarios privilegiados entre otros.
3.5011			LA solución SIEM debe permitir agregar indicadores de compromiso de manera automática desde una herramienta de análisis de malware avanzado con el objetivo de enriquecer las capacidades de análisis que posee la herramienta.
3.5012			La solución SIEM deberá permitir reducir falsos positivos y evaluar de forma dinámica el nivel de riesgo considerando la habilidad de unificar y correlacionar : · eventos, · información proveniente de herramientas de análisis de vulnerabilidades, y · criticidad de los activos o dispositivos.
3.5013			El motor de correlación de la solución SIEM, deberá estar basado en métodos de lógica booleana, reglas personalizables así como la detección de comportamiento anómalo mediante correlación estadística a través de cálculos de promedio. Adicionalmente la solución debe incluir reglas de correlación a nivel de seguridad preconfiguradas (Ej: Ataques de fuerza bruta)
3.5014			La solución SIEM deberá contar con una fórmula parametrizable que evalúe el nivel de riesgo de todos los eventos que son recibidos por el motor de correlación considerando los siguientes factores: · Importancia del evento · Criticidad del activo · Vulnerabilidades

3.5015			La solución SIEM deberá permitir la correlación de eventos entre distintos dispositivos (Cross Device Correlation) al almacenar todos los eventos recolectados en una única tabla dentro de su base de datos, independiente del tipo de dispositivo o aplicativo que la genere, permitiendo así la definición de contenido de correlación entre distintos tipos de dispositivos (firewalls, IDPs, Sistemas Operativos) sin la necesidad de utilizar estructuras complejas o lenguajes de acceso a datos para la consulta y unión de datos.
3.5016			La comunicación entre todos los componentes de la solución SIEM debe ser cifrada sin impactar en la performance. Deberá utilizarse al menos el algoritmo AES de 256 bits.
3.5017			La solución SIEM deberá proveer mecanismos para asegurar la integridad de los logs almacenados.
3.5018			La solución SIEM deberá ser capaz de ofrecer acceso a los logs almacenados históricos sin la necesidad de hacer una restauración de estos (restore).
3.5019			La solución SIEM deberá contar con un servicio de suscripción para la actualización y categorización de eventos durante la vigencia del contrato.
3.5020			La solución SIEM deberá soportar la integración de eventos provenientes de Active Directory, DHCP y concentradores VPN para monitorear la asignación de direcciones IP y asociar eventualmente los usuarios.
3.5021			La solución SIEM deberá integrarse con soluciones de gestión de vulnerabilidades. Detalle las soportadas.
3.5022			La interfaz de administración de la solución SIEM deberá ofrecer herramientas necesarias para el análisis de los eventos tales como "whois", "dig", "Nslookup", "Traceroute", etc.
3.5023			La solución SIEM deberá permitir la integración de dispositivos y aplicaciones de diferentes fabricantes (especificar con cuantas aplicaciones y fabricantes de terceros se integra), esto con el objetivo de evitar el desarrollo de los conectores.
3.5024			La solución SIEM debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente “fuera de la caja” (tales como aplicaciones o desarrollos hechos en casa) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos mediante un editor de expresiones regulares:

3.5025			Las herramientas para recolectar eventos de fuentes no soportadas deben proporcionar una interfaz que permita al equipo técnico de La institución realizar las configuraciones necesarias.
3.5026			El conjunto de herramientas para definir la lógica para extraer, obtener, normalizar y categorizar los eventos a correlacionar por la solución no deberán utilizar ningún lenguaje de programación JavaScript, Python o XML para definir la lógica de recolección de eventos. Únicamente se permitirá el uso de expresiones regulares o REGEX para definir patrones de búsqueda de cadenas de texto.
3.5027			La solución SIEM deberá tener la posibilidad de detectar actividad anormal en base a un línea de base detectando diferenciales
3.5028			Los componentes que realizan la recolección de eventos deberán utilizar el protocolo TCP como medio de transporte hacia la solución de correlación, verificando constantemente el estado de la conexión por medio de un pulso o “Heartbeat”. Ante la eventual pérdida de la conexión entre el componente de recolección y el motor de correlación, el primero deberá almacenar de forma inmediata los eventos bajo una cache de tamaño configurable hasta que se reanude dicha conexión, realizando la transmisión de los eventos hasta vaciar el cache.
3.5029			Los componentes de la solución SIEM que realizan la recolección de eventos deberán ofrecer la capacidad de ajuste en la hora de los eventos, en el caso de que el dispositivo que genere el evento no cuente con la hora correcta o no tenga configurado un servidor de NTP.
3.5030			La solución SIEM deberá poder integrarse con más de 600 distintos tipos de productos y dispositivos en forma nativa sin la necesidad de definir un proceso de colección a la medida.
3.5031			La solución SIEM deberá tener la capacidad de recibir logs en formato crudo (RAW) a través de los siguientes mecanismos: Syslog (TCP o UDP). Transferencia remota de archivos con log’s crudos por SCP (Secure Copy), sftp (Secure FTP) o ftp. Archivos de log’s en sistemas de archivos remotos mediante NFS y/o CIFS. OPSEC

3.5032			La solución SIEM deberá ser capaz de recibir eventos multi-línea y manejarlo como un solo registro. Se entiende por multi-línea aquellos eventos que se extienden a más de una línea, por ejemplo, registros de excepciones o errores.
3.5033			La solución SIEM propuesta deberá manejar niveles o tasas de compresión de eventos. (Describir e indicar el nivel de comprensión que ofrece la solución).
3.5034			El componente de recolección debe proveer mecanismos que garanticen la entrega de eventos y que los eventos no se pierdan si el sistema no está disponible. Debe poder almacenar eventos en un cache local durante una situación de falla en la red y entregar los eventos cuando el sistema vuelva a estar en línea.
3.5035			Debe ser posible implementar los componentes de recolección de eventos en Alta Disponibilidad (HA) en modalidad Activo/Pasivo
3.5036			La solución SIEM deberá capturar información a través de: Syslog, SNMPv2, SNMPv3, XML, OPSEC, WMI, RDEP, SDEE, Unix Pipe, API, Windows Event Logs transferencia de log's y eventos a través de FTP, SCP. Así mismo permitir la personalización para que también este disponible para fuentes únicas, como aplicaciones internas.
3.5037			La solución SIEM debe contar con módulo o componente de reportes que contenga plantillas predefinidas, basado en estándares internacionales. Posibilidad de manejar gráficos, tipo pie, barras, y otras características de personalización tañes como incluir los logos de la compañía.
3.5038			La solución SIEM debe permitir la gestión de incidentes de seguridad a través de funcionalidades de manejo de casos internos y workflow de incidentes.
3.5039			La solución SIEM debe poseer una base de datos creada especialmente para la gestión de grandes volumes de datos, es decir, no serán aceptadas bases de datos genéricas tales como Open Source (ex: MySQL/PostgreSQL) o Relacionales (Oracle y Microsoft SQL).
3.5040			La base de datos no debe requerir ningún tipo de mantenimiento por fuera de lo que el sistema ejecuta.
3.5041			La solución SIEM debe tener contenedores de paquetes de dashboards predefinidos, con el fin de facilitar la configuración de la herramienta y brindar visibilidad en el menor tiempo posible.

3.5042			Las alertas correlacionadas deben permitir usar parámetros como delta de eventos, con el fin de asociar cambios en la ocurrencia de los mismos.
3.5043			La solución SIEM deberá soportar la auditoría de usuarios autorizados en el sistema y registrar su actividad.
3.5044			La solución SIEM deberá soportar de forma nativa la integración con soluciones de almacenamiento en red como SAN, NAS, NFS o CIFS, para el almacenamiento de la información recolectada.
3.5045			La solución debe tener la funcionalidad de conectarse al sitio del fabricante para validar la existencia de nuevos contenidos. El contenido liberado debe tener la capacidad de agregar valor al monitoreo de la herramienta entregando distintos elementos adicionales tales como: - Reglas de correlación - Alarmas - Vistas (Dashboards) - Reportes - Variables - Listas de vigilancia.
3.5046			Como requisito “mínimo”, la solución debe contar con los siguientes componentes: - Componente de gestión, administración y operación de la solución. - Componente de recolección de eventos y/o log’s de seguridad. - Componente de recolección de flujos de red. Deberá soportar al menos Netflow v5, v7 y v9, J-flow, S-flow. - Componente de almacenamiento de eventos y/o log’s. - Agentes y conectores para recolectar eventos de seguridad de terceros. - Componente de reportes. - Componente de edición de parsers custom. - Componente de auditoría (registro de las actividades de los administradores y operadores de la solución.
3.5047			El sistema operativo de los equipos deberá estar previamente reforzado por el fabricante (hardening) para garantizar un adecuado desempeño de la solución.

3.5048			El o (los) appliance(s) deberá contar con mecanismos de redundancia, y tolerancia a fallas tales como fuentes de poder duales, configuración de arreglo de discos RAID; para garantizar la disponibilidad en el caso de presentarse alguna contingencia, garantizando la recolección continua de los log's y eventos de seguridad.
3.5049			La solución deberá contar con almacenamiento interno de 8TB neto utilizable para eventos en la base y 8TB neto utilizable para almacenamiento de eventos en crudo. El almacenamiento interno deberá estar configurado con RAID adecuado para garantizar su óptimo rendimiento. No se aceptará una configuración con RAID0.
3.5050			Con el objetivo de agilizar la entrega y búsqueda de información la arquitectura de la solución SIEM deberá contar con una parte de almacenamiento en discos de estado solido.
3.5051			La solución SIEM deberá permitir hacer un buen uso del almacenamiento mediante la compresión de eventos (1:14, 1:17 y 1:20)
3.5052			La solución SIEM deberá incluir una unidad de Storage Externo del tipo DAS (Directa Attached Storage) que cuente con al menos 10TB de almacenamiento neto.
3.5053			La solución SIEM debe estar en capacidad de respaldar 3 años de logs históricos. Se deben ofrecer los cálculos pertinentes para el dimensionamiento del almacenamiento.
3.5054			El componente de recolección debe manejar mecanismos de agregación que permitan disminuir el uso del ancho de banda. Deberá tener varios niveles de agregación y funcionar tanto para eventos como para flows.
3.5055			El componente de recolección debe permitir restringir el ancho de banda máximo utilizado en la red, el cual podrá ser definido en Kilobits por segundo (Kbps), Megabits por segundo (Mbps) o Gigabits por segundo (Gbps)
3.5056			La solución SIEM debe tener un manejador de severidad que le permita a los usuarios personalizar la criticidad de los eventos en múltiples niveles, realizando una ponderación que permita configurar dinámicamente la gravedad de un acontecimiento, o una serie de eventos, basándose en los valores de peso acostumbrados por la herramienta.

3.5057			La solución SIEM debe realizar automáticamente la generación de un mapa de calor, asociándole valores de riesgo cualitativo (Alto, Medio y Bajo) a los incidentes que se estén presentando en un período de tiempo determinado.
3.5058			La solución SIEM debe estar en capacidad de enlazar directamente fuentes externas como Bugtraq, ICE, CVE, Datastorm, MSDB y otros.
3.5059			La solución SIEM debe estar en capacidad de utilizar datos de vulnerabilidades recolectados desde herramientas externas para vincularlos a los a los eventos. Ya que los vínculos a dichas herramientas deben ser directos, deben actualizarse constantemente 24/7.
3.5060			La solución SIEM debe contar con mecanismos para realizar correlación basada en riesgo, si se llegara a requerir en un futuro por la organización.
3.5061			La solución SIEM debe permitir la carga de indicadores de compromiso, ya sea por otra solución del mismo fabricante o por bases de datos abiertas como Stix o TAXII, con el objetivo de posibilitar la configuración de alertas accionables a las ciber amenazas que se puedan presentar en el entorno de red.
3.5062			La solución SIEM debe permitir la configuración de listas negras, con el objetivo de posibilitar las respuestas accionables ante alertas correlacionadas.
3.5063			La solución SIEM debe estar en capacidad de comunicarse con bases de datos de reputación del mismo fabricante, con el objetivo de asociar parámetros como geolocalización a los parámetros de configuración de watchlists.
3.5064			La solución SIEM debe estar en capacidad de hacer push de scripts, como parte de las opciones de respuestas accionables.
3.5065			La solución debe permitir tomar indicadores de compromisos (IOC) desde fuentes rémoras para accesar actividad relacionada con estos en el ambiente de la organización.
3.5066			La solución debe contar con un módulo para realizar la retrospección (backtrace) de los indicadores de compromiso para evaluar la presencia en el ambiente de la organización.

3.5067			La solución debe integrarse de forma nativa a un sistema de reputación corporativo que permita conocer la reputación local, global o de análisis de la herramienta de Sandboxing de los programas ejecutables en los equipos monitoreados.
3.5068			La solución deberá integrarse al sistema de reputación corporativo a través de un protocolo de comunicación abierto multi-plataforma, que permita obtener el indicador de compromiso del archivo ejecutable analizado
3.5069			La solución permitirá importar indicadores de compromiso de fuentes externas a través de un lenguaje estructurado abierto para inteligencia de amenazas, tal como STIX.
3.5070			La solución SIEM deberá proporcionar un modulo integrado para la administración de eventos e incidentes de seguridad permitiendo asociar reglas a acciones tales como: · enviar una notificación al equipo de operadores. · abrir y asignar un caso a un usuario para su investigación. · ejecutar un script.
3.5071			La Solución SIEM deberá permitir una gestión completa de todos sus componentes, empleando una sola consola de administración, incluyendo todas las configuraciones de los dispositivos, configuración de políticas, gestión de eventos, informes, análisis, afinación de la solución, y otras funciones relevantes.
3.5072			La consola de administración centralizada debe proveer la configuración de controles de acceso basado en roles (RBAC) y permitir la configuración de privilegios de acuerdo a los perfiles asignados por el administrador de la solución. Permitiendo la segregación de funciones y acceso a eventos, obedeciendo al principio de mínimo privilegio.
3.5073			La Solución SIEM deberá contar con tableros gráficos de indicadores (dashboards) para el monitoreo de datos y eventos en tiempo real. Un tablero gráfico o dashboard deberá contener y agrupar una o más representaciones gráficas o tabulares de los datos bajo una misma vista permitiendo vistas tipo top 5, top 10 y top 20.

3.5074			La Solución SIEM deberá permitir desplegar más de un tablero gráfico (dashboards) de forma concurrente. Su actualización deberá ser en tiempo real sin la intervención del usuario o refresco manual. Desde el tablero de indicadores se debe tener la capacidad de visualizar los eventos base (drill down) y el detalle de cada evento.
3.5075			Los tableros gráficos (dashboards) de eventos deberán ser personalizables, editables y duplicables por los usuarios de la Solución de Correlación de Eventos.
3.5076			La solución SIEM deberá contar con dashboards predefinidos para regulaciones tipo PCI HIPPA ISO 27002 FISMA SOX Así como permitir la creación de grupos de Dashboards que ayuden a cumplimientos locales
3.5077			La solución debe contar con la capacidad de importar e instalar paquetes de contenidos que incluyan reglas de correlación, alarmas, vistas, variables y listas de monitoreo orientadas a casos de uso específicos que ayuden a responder a las amenazas existente de manera más eficiente.
3.5078			La solución SIEM deberá proporcionar una interface de administración gráfica (GUI) propia, para el personal operativo así como una interface de solo lectura diseñada para el personal de monitoreo y personal no técnico. Esta interfaz debe ser Web y segura (HTTPS)
3.5079			La solución SIEM deberá incluir una interface administrativa basada en Web segura (HTTPS) para la configuración, monitoreo, análisis y explotación de eventos, así como una interface de administración vía CLI (línea de comandos).
3.5080			La interfaz de administración gráfica de la solución SIEM deberá permitir la ejecución de aplicaciones o scripts externos bajo demanda, pudiendo incluso pasar parámetros o información de cada evento a herramientas de captura de paquetes de red (tcpdump), herramientas de geo-localización, traza de rutas (traceroute), búsquedas de dominios en whois.
3.5081			La solución SIEM deberá soportar un mecanismo de autenticación nativo además de soportar mecanismos alternativos como: Microsoft Active Directory, Autenticación de doble factor, LDAP , Radius.

3.5082			La solución SIEM deberá soportar autenticación y autorización mediante la definición de roles con privilegios granulares tanto para usuarios como para grupos. Los privilegios deben incluir: Agregar/Eliminar equipos Agregar/Eliminar políticas Gestión de Alarmas. Agregar/Eliminar/Editar alarmas Creación de reglas custom y variables Gestión de dispositivos Gestión de eventos
3.5083			La solución SIEM deberá ser capaz de enviar alertas vía email, mensajes SMS por protocolo SNMP así como notificaciones directas a usuarios de la misma consola de administración.
3.5084			La solución SIEM debe incluir contenido en modo de filtros, reglas predefinidas de correlación, monitores gráficos (dashboards) y reportes pre-configurados de monitoreo de dispositivos de red perimetral, enfocado a las mejores prácticas de seguridad y ataques más comunes.
3.5085			El fabricante de la solución deberá contar con servicios profesionales que eventualmente puedan desarrollar parsers a medida especialmente para La compañía
3.5086			El soporte técnico del fabricante deberá ser en modalidad 7x24 por chat, web y teléfono
3.5087			El soporte técnico del fabricante deberá incluir las actualizaciones de producto, firmas, nuevos releases y nuevas integraciones.
3.5088			Reporting
3.5089			La solución SIEM deberá ofrecer la capacidad de generar reportes calendarizados, con la opción de entrega por correo electrónico, publicación dentro de la misma solución, o almacenarlo localmente. Reportes de firewalls Reportes de administración de identidades. Reportes de IPS/IDS. Reportes de red Reportes de sistemas operativos Reportes de accesos Reportes de correlación de eventos
3.5090			La solución SIEM deberá ofrecer la capacidad de publicar reportes una vez que hayan sido ejecutados para que los reportes puedan ser consultados posteriormente sin necesidad de ejecutarlos nuevamente

3.5091			La solución SIEM deberá integrar reportes tipo drill-down, es decir, a partir de los resultados de un reporte, seleccionar algún resultado y automáticamente ser transferido a un nuevo reporte que proporcione un mayor nivel de detalle.
3.5092			El módulo de reportes, deberá permitir aceptar parámetros previos a la ejecución de un reporte, para poder focalizar los resultados del mismo. Ej.: Ingresar el nombre de usuario, nombre del dispositivo, etc.
3.5093			El módulo de reportes deberá permitir la visualización de un panel gráfico (dashboard), que agrupe múltiples elementos y permita desplegar resultados de reportes así como links externos. El dashboard deberá ser configurable e independiente para cada cuenta de usuario que utilice la solución.
3.5094			La solución SIEM debe contar con una base pre instalada de reportes, y permitir creación de reportes distribuidos en las siguientes categorías: Reportes PCI Reportes SOX Reportes de incidentes de seguridad Reportes de alertas de configuración del sistema Reportes por cada uno de las soluciones de seguridad integradas Reportes de múltiples dispositivos (cross-device)
3.5095			La solución SIEM deberá incluir todos los reportes y no deberá estar limitado en cuanto a términos de licenciamiento.
3.5096			La solución SIEM deberá contar con un módulo integrado para la ejecución de reportes sobre los eventos.
3.5097			Los reportes generados podrán ser de tipo ejecutivos (gráficos), detallados (matriz/tabla) o una combinación de ambos.
3.5098			El módulo de reportes, deberá permitir generar un reporte, ya sea desde cero, o bien, copiando y modificando reportes existentes.
3.5099			La solución SIEM deberá contar con funcionalidades integradas en la interfaz de administración gráfica para la definición, ejecución, programación y entrega automatizada de reportes ejecutivos y detallados en los siguientes formatos: PDF CSV HTML

3.6000	1	***Solución de Web Application Firewall, Application Delivery, Balanceador y Protección de DDOS***	**CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO**
3.6001			Los equipos ofertados debe ser una plataforma de hardware de propósito específico denominado "appliance".
3.6002			El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.
3.6003			Los valores de desempeño solicitados deberán ser logrados por el equipo "appliance" como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios "appliance" que logren sumar el valor solicitado.
3.6004			Se debe ofrecer dos (2) equipos en Alta disponibilidad funcionando en configuración de Par Activo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en clúster virtual de múltiples equipos.
3.6005			Cada equipo debe cumplir con las siguientes características:
3.6006			La solución debe soportar un Throughput en L4 de al menos 20 Gbps La solución debe soportar un Throughput en L7 de al menos 20 Gbps
3.6007			La solución debe soportar al menos 28 Millones de conexiones simultáneas La solución debe soportar al menos 250.000 conexiones por segundo en L4
3.6008			La solución debe soportar al menos 1 Millón de HTTP Requests por Segundo Cada equipo debe contar con al menos las siguientes Interfaces de red: Al menos 8 puertos SFP a 1Gbps

3.6009			Al menos 4 puertos SFP+ a 10 Gbps Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 110 a 220 VAC que se puedan remover en caliente (hot-swap) y certificadas 80 Plus Platinum" para eficiencia energética.
3.6010			Los equipos deberán ser instalados en rack estándar de 19", máximo 1RU.
3.6011			Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
3.6012			Cada equipo debe incluir 32 Gb de Memoria RAM mínimo
3.6013			Cada equipo debe incluir mínimo dos Disco duros de 500Gb en RAID 1
3.6014			Debe soportar clúster Activo/Activo y Activo/Pasivo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).
3.6015			La solución debe permitir configurar clúster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda
3.6016			Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.
3.6017			Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.

3.6018			La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.
3.6019			Los equipos deben tener hardware acelerador FPGA personalizables y programables para varias funciones como protección DDoS, protocolos SDN y manejo de trafico UDP
3.6020			FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO
3.6021			La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web (protocolos de capas superiores)
3.6022			La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
3.6023			La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.
3.6024			La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.
3.6025			Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones
3.6026			La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting:
3.6027			Round Robin Proporcional (Ratio)
3.6028			Proporcional dinámico Respuesta más rápida

3.6029			Conexiones mínimas Menor número de sesiones
3.6030			Tendencia de menor cantidad de conexiones Tendencia de desempeño
3.6031			Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM
3.6032			El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)
3.6033			El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
3.6034			La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica
3.6035			La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:
3.6036			Ping. Chequeo a nivel de TCP y UDP a puertos específicos
3.6037			Monitoreo http y https Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft.
3.6038			Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. Ejecución de scripts para determinar la respuesta emulando un cliente.
3.6039			Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma

3.6040			Monitoreo de aplicaciones de mercado: o LDAP o FTP o SMTP o IMAP/POP3 o Oracle o MSSQL o MySQL o RADIUS o SIP o Protocolo SASP o SOAP o WMI o SNMP Debe poder realizar todos estos métodos de persistencia de las conexiones: Dirección IP origen
3.6041			Dirección IP destino Cookies
3.6042			Hash SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia
3.6043			Sesiones SSL Microsoft Remote Desktop
3.6044			Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.
3.6045			Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.

3.6046			El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.
3.6047			Soporte de API para construir aplicaciones de administración o monitoreo personalizadas:
3.6048			Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados. Soporte de REST API Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts. Debe soportar el protocolo TDS para balanceo de MSSQL Debe soportar el protocolo NetFlow (v5 El sistema deberá soportar scripts de programación basados en un lenguaje estructurado (TCL) que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script. La solución debe permitir configuración de scripts basados en Node.js con el fin de brindar además del TCL, el acceso a paquetes de npm para facilitar la escritura y el mantenimiento del código. El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC 1.3 Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP. La Base de datos de geolocalización debe incluir los países de América Latina y estar disponible en el mismo

			equipo sin necesidad de acceso a Internet (offline). Incluir el soporte de Aceleración SSL usando Hardware Dedicado FUNCIONES DE SEGURIDAD GENERALES Cada equipo debe soportar seguridad SSL con las siguientes características:
3.6049			Incluir mínimo 10.000 Transacciones por segundo SSL (RSA 2K Keys) Soporte de llaves SSL RSA de 1024, 2048 y 4096 bits
3.6050			Soportar al menos 10 Gbps SSL Bulk Encryption (Thoughput SSL) Incluir mínimo 6.500 Transacciones por segundo SSL (ECDSA P-256)
3.6051			La solución debe soportar mirroring de sesiones SSL. Si el equipo primario falla el equipo secundario debe mantener la sesión SSL
3.6052			El Stack TLS del equipo debe soportar las siguientes funcionalidades/características
3.6053			Session ID Session Ticket
3.6054			OCSP Stapling (on line certificate status protocol) Dynamic Record Sizing
3.6055			ALPN (Application Layer Protocol Negotiation) Forward Secrecy
3.6056			La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECC)
3.6057			Debe soportar algoritmos de cifrado Camellia
3.6058			El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall)
3.6059			El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall
3.6060			Firmado criptográfico de cookies para verificar su integridad.

3.6061			Capacidad de integración con dispositivos HSM externos. Deberá soportar al menos Thales nShield Y Safenet (Gemalto) Luna.
3.6062			La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL.
3.6063			Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.
3.6064			Debe soportar HSTS (HTTP Strict Transport Security)
3.6065			Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.
3.6066			Scanners Exploits Windows
3.6067			Denial of Service Proxies de Phishing
3.6068			Botnets Proxies anónimos
3.6069			FUNCIONES DE ACELERACIÓN DE TRÁFICO
3.6070			La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de:
3.6071			Memoria cache. Compresión tráfico HTTP
3.6072			Optimización de conexiones a la aplicación a nivel TCP Multiplexación de conexiones hacia los servidores
3.6073			El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc.
3.6074			Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 6 Gbps o superior usando aceleración por Hardware dedicado, no la CPU de propósito general.
3.6075			Debe soportar el protocolo HTTP2 y funcionar como Gateway para este protocolo.

3.6076			Permitir la modificación de los tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los tags generados por el Web server o modificarlos
3.6077			Debe soportar Adaptive Forward Error Correction a nivel TCP y UDP
3.6078			DNS Y BALANCEO A DE ENLACES DE INTERNET
3.6079			La solución debe soportar el permitir alta disponibilidad de aplicaciones distribuidas en 2 o más datacenters, sin importar la ubicación geográfica.
3.6080			Debe funcionar como un servidor DNS autoritativo de alto desempeño, permitiendo manejar un dominio completo o delegación de parte de un dominio. Debe ser autónomo sin necesidad de balancear requerimientos DNS a una granja de servidores DNS.
3.6081			Debe funcionar como un servidor DNS cache autónomo, sin necesidad de balancear requerimientos DNS a una granja de servidores.
3.6082			Para el balanceo global (DNS), debe permitir los siguientes métodos de balanceo estático y dinámico, de manera nativa y no a través de configuración por scripting:
3.6083			Round Robin Global Availability
3.6084			Geolocalización Capacidad del Servicio
3.6085			Least Connections Packets Per Second
3.6086			Round Trip Time Drop Packet
3.6087			Hops Packet Completion Rate
3.6088			User-defined QoS Proporcional (Ratio)
3.6089			Kilobytes Per Second Regreso al DNS
3.6090			Persistencia estática Puntuación del Servicio

3.6091			Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo datacenter por el transcurso de su sesión.
3.6092			Permitir Balanceo de cargas ente datacenters de acuerdo a la ubicación geográfica
3.6093			Debe permitir la creación de topologías personalizadas con el fin de permitir distribución de tráfico basado en requerimientos particulares de la infraestructura
3.6094			Debe permitir monitoreo de la infraestructura y las aplicaciones a balancear, integrándose con otros equipos del mismo fabricante o de terceros.
3.6095			Las zonas del DNS Autoritativo deben cargarse en RAM, para evitar latencias y tener tiempos de respuesta rápidos.
3.6096			Debe permitir realizar balanceo de servidores DNS.
3.6097			Debe soportar el protocolo DNSSEC
3.6098			Debe incluir herramienta de administración grafica para el manejo de zonas DNS
3.6099			Debe soportar registros AAAA para IPv6
3.6100			Debe soportar traducción entre DNS IPv4 y DNS IPv6
3.6101			La solución debe soportar 480.000 respuestas DNS por segundo.
3.6102			La solución debe permitir balanceo de enlaces de internet, sin restringir el numero de enlaces y sin importar el proveedor de estos.
3.6103			Debe proveer balanceo de tráfico saliente entre múltiples ISP y detectar el fallo de alguno de ellos para enrutar automáticamente el tráfico hacia los demás ISP.
3.6104			Debe proveer balanceo de trafico entrante, basado en DNS y responder autoritativamente a queries DNS tipo A
3.6105			Debe permitir monitoreo de los enlaces y detectar fallos en ellos.
3.6106			Debe manejar persistencia a nivel global, manteniendo a los usuarios en un mismo ISP por el transcurso de su sesión
3.6107			FUNCIONES DE FIREWALL Y PROTECCION DDOS
3.6108			Debe incluir protección contra ataques de DDoS en capas 2-4 utilizando vectores de ataque personalizables
3.6109			La solución de DDoS debe contar con un sistema de protección basado en comportamiento (Behavioral) que permita la creación de firmas o vectores de ataque de manera dinámica.

3.6110			La solución debe proteger contra ataques de denegación de servicio tanto en una topología en línea (inline deployment) como en una topología fuera de línea (TAP mode)
3.6111			Debe bloquear ataques a nivel de red como flood, sweep, teardrop, smurf attacks
3.6112			Debe mitigar ataques basados en protocolos, incluyendo SYN, ICMP, ACK, UDP, TCP, IP, DNS, ICMP, ARP
3.6113			Debe permitir la creación de reglas basadas en aplicación, independientes para cada una de ellas.
3.6114			Debe permitir la creación de reglas globales.
3.6115			Debe tener la opción de funcionar como un firewall statefull full-proxy y ser certificado por ICSA Labs como Network Firewall
3.6116			Debe permitir la definición de horarios (schedules) que apliquen a las reglas configuradas, permitiendo activar reglas
3.6117			Entre intervalos de tiempo
3.6118			Hasta una fecha especifica
3.6119			Después de una fecha específica.
3.6120			Debe permitir la creación de listas blancas (White lists) de direcciones IP
3.6121			Debe permitir la configuración de túnel IPSEC Site-to-Site
3.6122			Debe incluir funcionalidad de application delivery controller o integrarse con dispositivos de Application Delivery
3.6123			Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo DNS, poder controlar el tráfico DNS de acuerdo al tipo de Registro solicitado y detectar anomalías a nivel del protocolo
3.6124			Debe brindar protección contra Ataques de Denegación de Servicio para el protocolo SIP y poder controlar el tráfico SIP de acuerdo al Método SIP recibido y detectar anomalías a nivel del protocolo
3.6125			Debe permitir personalizar los Logs, y ser exportados a un repositorio Syslog externo que conste de uno o varios servidores.
3.6126			Debe funcionar como un Proxy SSH para control de conexiones entre diferentes redes con el fin de dar visibilidad a las sesiones SSH y controlar las mismas

3.6127			Debe soportar Port Misuse, evitando que servicios pasando a través de puertos conocidos que buscan saltar protecciones de Firewall (por ejemplo un servicio SSH escuchando en el puerto 80 y busque abusar de reglas orientadas a HTTP).
3.6128			Debe soportar RTBH (Remotely Triggered Black-hole Route Injection) para protección en caso de implementaciones fuera de línea.
3.6129			Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT
3.6130			ESTÁNDARES DE RED
3.6131			Soporte VLAN 802.1q, Vlan tagging
3.6132			Soporte de 802.3ad para definición de múltiples troncales
3.6133			Soporte de NAT, SNAT
3.6134			Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
3.6135			Soporte de Rate Shapping.
3.6136			Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
3.6137			Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.
3.6138			Debe soportar el protocol de OVSDB (Open vSwitch Database) para crear túneles VXLAN usando un controlador SDN
3.6139			Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS
3.6140			ADMINISTRACIÓN DEL SISTEMA
3.6141			La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH, interfaz de administración gráfica basada en Web seguro (HTTPS)
3.6142			La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.
3.6143			La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.

3.6144			La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
3.6145			La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
3.6146			La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante:
3.6147			Protocolo SysLog Notificación vía SMTP
3.6148			SNMP versión.2.0 o superior. El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico. El equipo debe contar con un módulo de administración tipo lights out que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque. La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos. Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (ej, Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.
3.7000	1	***Solución de Anti-Spam***	Solución capaz de implementarse en appliance con capacidad de ser soportada también en entorno virtual (ESX) como combinación de ambas o completamente como opción en la nube (SaaS) provistas por el mismo fabricante.

3.7001			El appliance debe contar con arreglos RAID y capacidad mínima de 250GB en disco duro. Debe ofrecerse una solución de alta disponibilidad
3.7002			Contar con tarjetas de red 10/100/1000 con capacidad de bounding para alta disponibilidad.
3.7003			Contar con al menos 8 GB de RAM con posibilidad de expansión.
3.7004			Soporte al hardware disponible en la región por el fabricante del mismo.
3.7005			Sistema operativo robustecido e integrado con la solución.
3.7006			Administración vía HTTPS y SSH.
3.7007			Capacidad de configurar los appliance en modo de alta disponibilidad.
3.7008			Gestión centralizada en configuración de alta de disponibilidad.
3.7009			Capacidad de separar funcionalidades por instancia.
3.7010			Debe soportar procesamiento nativo de SMTP sin PROXY reverso a otros protocolos.
3.7011			Si la solución es SaaS se debe contar con la certificación SAS70 para los sites de procesamiento como mínimo.
3.7012			Esquema de alta disponibilidad para sitios SaaS con redundancia geográfica.
3.7013			La solución debe ser la misma en cualquier tipo de implementación.
3.7014			La configuración en appliance debe permitir ejecutar todos los engines sin precisar de plataformas adicionales o de terceros.
3.7015			la Solución debe ser capaz de integrarse con cualquier plataforma de Mensajería, ejemplo Microsoft Exchange en al menos sus 3 ultimas versiones.
3.7016			La solución debe contar con un sistema de reputación propietario no dependiente del resto de los engines de detección.
3.7017			La detección de trafico malicioso debe poder realizarse en ambas direcciones, permitiendo el control e identificación de ataques internos.
3.7018			La solución deberá permitir identificar amenazas mediante puntajes de los distintos engines a través de la correlación de los mismos.
3.7019			La solución debe permitir la modificación de los umbrales de detección de acuerdo a las necesidades de la empresa, así como la creación de perfiles para distintas rutas, dominios, usuarios o direcciones IP.

3.7020			Los engines de detección deben actualizarse regularmente y las actualizaciones deben ser descargadas del site del fabricante una vez probados para evitar cualquier impacto al trafico.
3.7021			Los engines de detección deben ser configurables de forma independiente para poder tropicalizarlos a los requerimientos de la empresa
3.7022			La Solución debe poderse configurar para bloquear correos de marketing o similares (Bulk Mail).
3.7023			La Solución debe poder configurar listas blancas y negras para los engines de Anti-Spam, tanto a nivel General como individual de así precisarse.
3.7024			Se debe contar con un engine que permita que el administrador genere reglas para mensajes específicos tanto permisivos como restrictivos que hagan override a las reglas estándar definidas por la solución.
3.7025			Las políticas de control de SPAM deben ser modificables.
3.7026			Las reglas o políticas de bloqueo deben poder configurarse desde una sola ventana o interfaz.
3.7027			Debe contar con soporte para DKIM
3.7028			Debe contar con soporte para SPF
3.7029			Debe soportar con soporte para DMARC
3.7030			Debe contar con una herramienta para bouncing que permita llaves fijas y dinámicas.
3.7031			Debe poseer la funcionalidad de control de SMTP para controlar ataques tanto internos como externos.
3.7032			Poseer integración con directorio activo o bases de datos para verificación de usuarios.
3.7033			La herramienta debe contar con reportes a usuario final que permitan tomar acciones como liberar o notificar spam, vía correo electrónico o bien a través de un portal de usuario.
3.7034			Las opciones de las notificaciones a usuario final deben poder ser configurables por el administrador para restringir o habilitar funcionalidades.
3.7035			Debe contar con áreas de cuarentena especificas por engine.
3.7036			El modulo debe tener la capacidad de configurarse para distintas rutas, direcciones y dominios.
3.7037			Acceso a la consola vía HTTPS y SSH
3.7038			Gestión de administradores por niveles y perfiles de acceso.
3.7039			Passwords administrativos configurables para cumplir los requerimientos de la empresa.

3.7040			Gestión de puertos para control de acceso a los administradores y usuarios.
3.7041			Debe contar con la opción de enviar y recibir correo cifrado de dominio a dominio a través de TLS/SSL y permitir agregar los certificados públicos de dominios confiables.
3.7042			Debe contar con un reporte de utilización del equipo por engine.
3.7043			Debe contar con un reporte de que muestre el estado de cada equipo que conforma la solución.
3.7044			Debe contar con un sistema de alertas que permita monitorear el estado del equipo.
3.7045			Debe permitir la interacción a través de traps para integración con sistemas de monitoreo
3.7046			La solución debe contar con una herramienta de búsqueda de correos que permita ver el estado de cada correo procesado y que permita ver información a nivel forense, debe estar integrada al costo de la solución.
3.7047			La solución debe contar con un engine para poder hacer cumplimiento con reglamentaciones como SOX, HIPPA, GLBA, PCI, etc.
3.7048			La solución debe contar con contenedores para identificadores de cada uno de los cumplimientos descritos y estos deben actualizarse de existir modificaciones a las regulaciones de forma automática
3.7049			La solución debe contar con un repositorio de socios de negocio, que permita identificar a las empresas que precisan de ciertos cumplimientos.
3.7050			La solución debe contar con reglas que permitan parametrizar y ajustar cada uno de los cumplimientos en función de las necesidades de la empresa
3.7051			Debe permitir la utilización de diccionarios específicos para cumplimientos de reglamentaciones locales o especificas.
3.7052			La gestión de políticas para la aplicación de las reglas de cumplimiento deben ser granulares.
3.7053			Las solución debe contar con una sección especifica de DLP en la cual se pueda ver un sumario de las violaciones a las políticas.
3.7054			Debe poseer folders específicos para identificación de violaciones, uno por cada política existente.
3.7055			Debe contar con un área de búsqueda de incidentes que permita ubicar por distintos argumentos los mensajes.

3.7056			La herramienta debe contar con un engine que permita identificar si algún documento clasificado como confidencial es enviado a través del correo, debe tener la capacidad de identificar el documento completo o partes del mismo.
3.7057			El engine debe poder ser configurado para solo permitir que usuarios autorizados envíen la información y debe poder tomar distintas acciones para las incidencias.
3.7058			La solución debe poder almacenar los documentos en categorías, y los documentos deberán poder ser ingresados o de forma directa o a través de conexión con los resguardos definidos.
3.7059			La solución debe contar con un engine que permita el cifrado de correos salientes.
3.7060			El cifrado debe ser transparente para los receptores, esto es no, debe usar ningún tipo de agente o conexión con el sistema.
3.7061			La gestión de las llaves debe ser provista en la nube, no debe depender del equipo emisor.
3.7062			La solución debe permitir al administrador revocar, delimitar en tiempo y eliminar usuarios lectores.
3.7063			La solución debe contar con un portal de auto-gestión para los receptores de correo cifrado.
3.7064			La solución podrá funcionar sola o en combinación con las reglas definidas para el trafico con el resto de los módulos.
3.7065			Los correos cifrados emitidos deben poder ser vistos en dispositivos móviles.
3.7066			La herramienta debe poder permitir, de ser necesario, que los usuarios receptores puedan enviar correos a la institución usando la misma herramienta.
3.7067			Capacidad de integrar archivo de correos en la nube
3.7068			Capacidad de compartir archivos grandes de forma cifrada
3.7069			La solución debe estar dentro del cuadrante de lideres de Gartner y Forester.
3.8000	1	***Solución de Web Content Filtering***	Solución de filtrado de contenido Web, que incluye funcionalidades nativas integradas de: filtrado URL, control de aplicaciones Web, antimalware y prevención de fuga de información (DLP).
3.8001			Solución de filtrado de contenido Web, basado en apliances (físicos y/o virtuales) de tipo gateway, por lo que no se aceptará software instalado en servidores.

3.8002			La solución deberá estar basado en un sistema operativo propietario, no se aceptarán soluciones basados en sistemas operativos genéricos como Windows o Linux.
3.8003			La solución permite inspeccionar el trafico tanto de entrada como de salida de los protocolos HTTP, HTTPS y FTP.
3.8004			La solución deberá permitir la inspección del tráfico SSL, HTTPS de forma que pueda analizar sobre este protocolo para la identificación de malware.
3.8005			La solución deberá permitir descifrar el tráfico SSL para escanearlos y luego volver a cifrarlo antes de enviar al usuario
3.8006			La solución deberá soportar terminación SSL para pedidos HTTPS
3.8007			La solución deberá contar con un motor Antimalware basado en firmas y comportamientos.
3.8008			La solución deberá contar con múltiples motores de protección.
3.8009			La solución deberá permitir el bloqueo de contenido que contenga virus, spyware, botnets y malware.
3.8010			La solución deberá permitir la detección heurística proactiva.
3.8011			La solución deberá permitir la detección de malware entrando y saliendo de la red.
3.8012			Las firmas deberán ser actualizadas automáticamente o bajo demanda de los administradores.
3.8013			El escáner proactivo deberá inspeccionar en profundidad el HTML y el código script utilizado por URLs hostiles, explotación de buffer overflow y shellcode injection.
3.8014			La solución deberá permitir el filtrado de URL basado en categorías, para ello la solución deberá contar con mas de 100 categorías pre-definidas.
3.8015			La solución deberá permitir el bloqueo de mensajería instantánea (IM)
3.8016			La solución deberá permitir el bloqueo de aplicaciones Peer-to-Peer
3.8017			La solución deberá permitir el bloqueo de Streaming Media
3.8018			La solución deberá contener la base de datos de sitios web

3.8019			La solución deberá permitir el filtrado basado en reputación de los sitios web, para ello deberá contar con un sistema de reputación "en la nube" administrado y mantenido por el mismo fabricante que permita bloquear de forma dinámica contenido Web malicioso
3.8020			La solución deberá permitir la utilización de listas negras y listas blancas
3.8021			La solución deberá contar con protección contra sitios web sin categorizar
3.8022			La solución deberá tener la capacidad de filtrado por:
3.8023			• Revisión por reputación de archivos
3.8024			• Tamaño del archivo
3.8025			• Extensión del archivo
3.8026			• Encabezados
3.8027			• Usuario o Grupo que realiza la descarga
3.8028			La solución deberá analizar en tiempo real una página y basándose en el contenido de la misma y catalogarla en tiempo real.
3.8029			Las actualizaciones de contenido para el filtrado de URL deberán actualizarse diariamente
3.8030			Las actualizaciones de los filtros por reputación de URL deben actualizarse en tiempo real continuamente, inmediatamente después que hayan sido descubiertas por el fabricante.
3.8031			La solución deberá permitir el Control de mas de 1,000 Aplicaciones Web, permitiendo el control granular de características de aplicaciones tales como Facebook, Twitter, entre otras.
3.8032			La solución deberá tener la habilidad de remover de los sitios web contenido seleccionado por los administradores del sistema, eliminando o removiendo código del sitio, para que no sea presentado al usuario final.
3.8033			La solución deberá permitir el filtrado de tráfico no HTTP, como puede ser el de los programas P2P (eMule, etc.) o IM (mensajería instantánea).
3.8034			La solución deberá identificar el tipo de servicio o aplicación aprovechando la capacidad de realizar filtrados o análisis por cadenas o “body” dentro del código HTML de las páginas o sitios invocados.

3.8035			La solución deberá contar con un módulo de prevención de pérdida de datos (DLP) que analice la información que sale desde la red interna. Deberá buscar palabras claves dentro de los REQUEST de http. Estas palabras claves pueden se deberán alimentar en diccionarios que sean modificables por la ACP.
3.8036			La solución deberá buscar información especificada en las clasificaciones de las reglas apropiadas. Si el módulo encuentra un texto especificado, se disparará una acción por parte del sistema.
3.8037			La solución deberá poder mantener diccionarios que disparen acciones por parte del sistema.
3.8038			La solución deberá ser ofertada en una configuración de Clustering Activo-Activo permitiendo así el balaceo de carga entre al menos dos (02) equipos.
3.8039			La solución deberá enviar alertas para eventos críticos relacionados con hardware o software del producto a los administradores del sistema.
3.8040			La solución deberá soportar al menos 1200 usuarios, escalable. En caso requerir licencias estas deberán estar incluidas para toda la solución propuesta.
3.8041			Permite desplegar la solución de forma flexible ya sea en appliances físicos y/o virtuales de acuerdo a las necesidades y crecimiento de la institución, sin necesidad de requerir licencias adicionales para el despliegue de uno u otro modo, solamente las requeridas para cubrir la cantidad de usuarios solicitada.
3.8042			Deberá permitir desplegarse la solución "en la nube" para 100 usuarios usuarios que se encuentren fuera de la red corporativa pero que puedan mantener las mismas políticas corporativas, para ello estas políticas se deberán configurar en la misma consola de administración de la herramienta.
3.8043			La solución debe soportar los siguientes modos de configuración:
3.8044			• Proxy Explícito
3.8045			• Proxy (Standalone Proxy)
3.8046			• Proxy con WCCP (Foward Proxy)
3.8047			• Proxy con ICAP
3.8048			• Transparent Bridge (Proxy Transparente)
3.8049			• Transparent Router (Proxy Transparente)
3.8050			La solución deberá soportar proxy SOCKS
3.8051			La solución deberá soportar otros proxys opcionales como FTP

3.8052			La solución deberá soportar un mínimo 500 Mbps de trafico Internet escalable a 1 Gbps, en caso de que la solución propuesta sea en clúster, se deberán incluir los equipos necesarios para garantizar el trafico de Internet solicitado. Los equipos tienen que tener la capacidad de manejar todo el tráfico aún en la situación donde alguno de ellos se encuentre no operacional.
3.8053			La solución deberá soportar un mínimo de 50,000 request/segundo de trafico Web, en caso de que la solución propuesta sea en clúster, se deberán incluir los equipos necesarios para garantizar los request/segundo de trafico Web aún en la situación donde alguno de ellos se encuentre no operacional.
3.8054			La Solución debe poder recibir y enviar reputaciones de Hash en tiempo real mediante un protocolo destinado a ello
3.8055			La solución debe permitir integrarse de forma transparente a una solución de detección de malware avanzado a través de diversas técnicas de detección incluyendo sandbox, para lo cual el equipo de seguridad Web deberá enviar el archivo a analizar a la solución de detección de malware avanzado a través de la red.
3.8056			La solución debe permitir detener el ataque detectado a través de la solución de detección de malware avanzado de forma inmediata y sin intervención del administrador.
3.8057			Debe permitir integrar de manera nativa el análisis externo de fuga de información mediante appliance DLP a nivel de red, para lo cual el equipo deberá enviar mediante protocolo ICAP el elemento el cual debe ser analizado.
3.8058			La solución debe administrarse desde una única consola grafica basada en Web en equipos Windows o Linux con navegadores Microsoft Internet Explorer (Windows) y Mozilla Firefox (Windows/Linux)
3.8059			La solución debe permitir la administración central de 2 o más appliances sin la necesidad de agregar equipos adicionales
3.8060			La solución deberá soportar la conexión para administración bajo protocolos SSH o SCP.
3.8061			La solución deberá poder realizar respaldos y restauraciones de las configuraciones.
3.8062			Integración con las soluciones complementarias de análisis de malware avanzado y reputación de archivos en real time del mismo fabricante

3.8063			La solución deberá poder integrarse con un Active Directory de Microsoft sin necesidad de instalar algún componente en los controladores de dominio. Esta integración permitirá que la administración de la solución se efectué por medio de cuentas de usuarios y grupos de administración basadas en el Active Directory.
3.8064			Administración Basada en Roles: Es requisito indispensable que se pueda segregar la administración de la seguridad diferenciando claramente los roles de Seguridad del de Sistemas y de otras unidades definidas en el Active Directory. La solución deberá permitir la segregación de funciones de forma granular, permitiendo así definir al alcance o posibilidades de gestión para cada administrador.
3.8065			La solución tendrá la capacidad de presentar al usuario, una página web con mensajes modificables por los administradores del sistema, en caso de algún problema o infracción.
3.8066			La solución deberá permitir el control de cuotas para los usuarios por ancho de banda
3.8067			La solución deberá permitir el control de cuotas para los usuarios por tiempo consumido
3.8068			La solución deberá permitir el control de cuotas de tamaños de los archivos
3.8069			La solución deberá tener la capacidad de utilizar expresiones regulares para la creación de las políticas
3.8070			La solución deberá tener la capacidad de utilizar expresiones booleanas para la creación de políticas
3.8071			La solución deberá tener la capacidad de utilizar las políticas en forma anidadas o encadenadas
3.8072			Las políticas de Accesos deberán estar basadas en:
3.8073			• Dirección IP
3.8074			• Rango de Direcciones IP
3.8075			• Subredes y CIDR
3.8076			• Usuarios del Active Directory
3.8077			• Grupos de Usuarios del Active Directory
3.8078			La solución deberá soportar la configuración de tiempos de conexión mediante la configuración de reglas específicas.
3.8079			Los usuarios móviles deben poder autenticarse a aplicaciones en la nube por SSO
3.8080			La solución deberá permitir generar reportes en tiempo real
3.8081			La solución deberá permitir generar reportes históricos

3.8082			La solución deberá permitir generar reportes de actividad de los usuarios
3.8083			La solución deberá permitir generar reportes de los sitios bloqueados
3.8084			La solución deberá tener la capacidad de enviar reportes programados por correo electrónico
3.8085			La solución deberá permitir exportar los reportes generados en los siguientes formatos al menos: PDF, HTML, XML y CSV.
3.9000	1	***Solución de Network Access Control (NAC)***	La solución de NAC ofertada debe permitir manejar los 1000 dispositivos de la red simultáneamente en una plataforma de alta disponibilidad
3.9001			La solución de Control de Acceso a la Red deberá ser instalada dentro de la infraestructura de la institución. La administración y gestión de la solución deberá permitir ser gestionada de manera centralizada.
3.9002			Esta solución será implementada para resguardar dispositivos finales, servicios y aplicaciones que se encuentran en las oficinas de la institución y se encargará de la protección y definición de políticas para control del acceso a la red e infraestructura de la institución.
3.9003			Todos los componentes que constituyan la "Solución de Control de Acceso a la Red" deberán ser del mismo fabricante.
3.9004			La "Solución de Control de Acceso a la Red" deberá ser ofertada con licenciamiento, garantías, mantenimiento, actualización, servicios de instalación y soporte técnico del fabricante para tres (3) años en todos sus componentes, esto a partir del acta entrega recepción del proyecto.

3.9005			El funcionamiento general buscado es el siguiente: Cuando un usuario requiere acceder a la red corporativa mediante su equipo de escritorio o móvil (Laptop, Tablet, Smartphone), luego de encenderse e intentar conectarse a la red debe solicitarse al usuario las credenciales de acceso, si estas son válidas, se comprobará el estado del equipo. Si el usuario es válido y tiene permiso de acceso y el equipo cumple con los elementos de software y configuraciones mínimas requeridas, se le habilitará el acceso a la red corporativa (e.j. asignación de VLAN). Si el usuario es válido pero el equipo no cumple, se lo conectará a una red de remediación y se dispararán automáticamente los procesos de remediación para luego realizar la validación nuevamente. Si el usuario no es válido o no cuenta con el software para validarse, se lo conectará a una red de visita que ofrecerá algunos servicios básicos como por ejemplo acceder a Internet.
3.9006			En caso de no tenerse instalado el software requerido para la validación, el mismo podrá ser descargado de un portal que habilitará al usuario a autenticarse y validar su equipo posibilitándosele el acceso como se describió anteriormente. Adicionalmente, debe cumplir con las siguientes características:
3.9007			Control de acceso a la red agnóstico a la infraestructura de red cableada e inalámbrica (redes heterogéneas).
3.9008			Alta Disponibilidad: contar con infraestructura replicada que pueda ser instalada en ubicaciones diferentes
3.9009			Autenticación y Autorización: para esto debe ofrecer integración nativa con Radius, Active Directory y/o LDAP, que permita autorizar los accesos basado en la pertenencia de usuarios a grupos del Directorio Corporativo.
3.9010			Soporte para el protocolo IEEE 802.1X
3.9011			Asignación dinámica de VLAN's de Seguridad y/o Remediación creadas en la red.
3.9012			No debe bloquear a los usuarios fuera de la red, si no ofrecerles un acceso de remediación a una VLAN de visitantes
3.9013			Notificaciones automatizadas a los usuarios sin requerir involucramiento del staff técnico.
3.9014			La detección y aislamiento debe ser agnóstico al hardware y sistema operativo de los dispositivos

3.9015			Soporte para aplicar políticas a través de redes cableadas, inalámbricas y VPN
3.9016			Soporte para análisis de elementos de software instalados y configuración de la frecuencia de revisión.
3.9017			En caso de operar sin agente, deberán mencionarse los alcances y requerimientos de esta modalidad.
3.9018			Agente: En caso de contar con un agente permanente para eficientizar la validación de elementos de software, deberá tener un mecanismo propio mediante la consola o mediante un tercero, para la distribución del cliente
3.9019			Cliente (Agente) Temporal: Para estos casos, el cliente no deberá exigir un pre-requisito sobre las credenciales del usuario (ej. requerir permisos especiales sobre el sistema)
3.9020			Portal cautivo: A través de este portal es que se dejará disponible para los usuarios que lo requieran, la descarga del "cliente temporal" el cual les permitirá validarse y chequear la postura del equipo para posibilitarles el acceso.
3.9021			Debe ofrecer o re-direccionar a un portal con información de la remediación para el usuario final
3.9022			Debe tener la flexibilidad de crear excepciones personalizadas de forma granular en sus políticas para toda la comunidad de usuarios
3.9023			Control mediante un número máximo de MACs por puerto (nodo de red) en aquellos que no están dedicados a extender la red (para evitar que instalen hub y switches sin autorización)
3.9024			Para las redes cableadas, debe cumplir con lo siguiente:
3.9025			La solución de NAC debe revisar los criterios de postura y compliance.
3.9026			Validar pertenencia del dispositivo a la red corporativa mediante alguna de las siguientes posturas:
3.9027			Certificado digital instalado en el equipo. Archivo almacenado en el file system del equipo.
3.9028			Programa instalado o en ejecución. Entrada en el registro del sistema "regedit" con un valor determinado.

3.9029			Registro del equipo en el Active Directory corporativo. Validación periódica: El sistema debe proveer un mecanismo que permita la revalidación de la postura del equipo periódicamente, de forma que si las políticas cambian o la configuración del equipo cambia, podrá cambiar su condición debiéndose actualizar los accesos habilitados al usuario. En caso de ocurrir un cambio, debe ser notificado el usuario a través de un mensaje informativo en la pantalla de su equipo. El tiempo de revalidación debe poder ser configurable.
3.9030			Requerimientos de elementos:
3.9031			Firmas y Motor del Anti-Virus con un máximo de N" días de obsolescencia
3.9032			Firmas y Motor del Anti-Spyware con un máximo de N" días de obsolescencia
3.9033			Validación de Firewall en el host activo Revisión de parches del Sistema Operativo
3.9034			Validación de Full Disk Encryption (si el agente está instalado y activo) Validación de Aplicaciones en general (si el agente está instalado y activo)
3.9035			Para dispositivos no administrados: Esta categoría incluye, sin estar limitada a, Impresoras, Escáneres, Switches para BYOD y Access Points:
3.9036			Soporte para Control de dispositivos BYOD, VLAN de Visitantes con Acceso Limitado a Internet o Aplicaciones (Web,SSL,etc.)
3.9037			Habilidad para bloquear dispositivos no autorizados que soliciten direccionamiento al servidor de DHCP
3.9038			Soporte para detectar Sistemas Operativos Independientes (sin Agente)
3.9039			Validación periódica: El sistema debe proveer un mecanismo que permita la revalidación de la postura del equipo periódicamente, de forma que si las políticas cambian o la configuración del equipo cambia, podrá cambiar su condición debiéndose actualizar los accesos habilitados al usuario. En caso de ocurrir un cambio, debe ser notificado el usuario a través de un mensaje informativo en la pantalla de su equipo. El tiempo de revalidación debe poder ser configurable.

3.9040			Habilidad para solicitar las credenciales de acceso vía un portal web a los visitantes (portal cautivo), aislándolos en una VLAN limitada para visitantes.
3.9041			Red Inalámbrica
3.9042			Para dispositivos administrados: Esta categoría incluye, sin estar limitada a, Laptops, Tabletas y Teléfonos Inteligentes
3.9043			La solución de NAC debe revisar los criterios de postura y compliance.
3.9044			Soporte para dispositivos móviles (Tablet, Smartphone, Laptop). Sistemas Android, IOS, Windows, etc
3.9045			Validar pertenencia del dispositivo al corporativo, mediante alguna de las siguientes posturas:
3.9046			Certificado digital instalado en el equipo. Archivo almacenado en el file system del equipo.
3.9047			Programa instalado o en ejecución. Entrada en el registro del sistema "regedit" con un valor determinado.
3.9048			Registro del equipo en el Active Directory corporativo. Validación periódica: El sistema debe proveer un mecanismo que permita la revalidación de la postura del equipo periódicamente, de forma que si las políticas cambian o la configuración del equipo cambia, podrá cambiar su condición debiéndose actualizar los accesos habilitados al usuario. En caso de ocurrir un cambio, debe ser notificado el usuario a través de un mensaje informativo en la pantalla de su equipo. El tiempo de revalidación debe poder ser configurable.
3.9049			Requerimientos de postura de elementos de software:
3.9050			Firmas y Motor del Anti-Virus con un máximo de N" días de obsolescencia
3.9051			Firmas y Motor del Anti-Spyware con un máximo de N" días de obsolescencia
3.9052			Validación de Firewall en el host activo Revisión de parches del Sistema Operativo
3.9053			Validación de Full Disk Encryption (si el agente está instalado y activo) Validación de DLP (si el agente está instalado y activo)

3.9054			Para dispositivos no administrados: Esta categoría incluye, sin estar limitada a, Laptops de Invitados, BYOD de Empleados, Teléfonos Inteligentes desconocidos y dispositivos inalámbricos desconocidos.
3.9055			Habilidad para solicitar las credenciales de acceso vía un portal web a los visitantes (portal cautivo), aislándolos en una VLAN limitada para visitantes.
3.9056			Detección independiente al Sistema Operativo, cualquier sistema puede ser detectado y controlado por la política
3.9057			Habilidad para dar tratamiento a dispositivos que no se han validado (BYOD)
3.9058			Validación periódica: El sistema debe proveer un mecanismo que permita la revalidación de la postura del equipo periódicamente, de forma que si las políticas cambian o la configuración del equipo cambia, podrá cambiar su condición debiéndose actualizar los accesos habilitados al usuario. En caso de ocurrir un cambio, debe ser notificado el usuario a través de un mensaje informativo en la pantalla de su equipo. El tiempo de revalidación debe poder ser configurable.
3.9059			La solución ofertada debe ofrecer las siguientes capacidades para reportes, monitoreos y gestión:
3.9060			La consola debe tener un Tablero de Control (Dashboard) que muestre los avisos más relevantes
3.9061			Generación de reportes orientados a compliance: SOX, COBIT, PCI/DSS, LFPDPPP, etc.
3.9062			Debe reportar un inventario de dispositivos de usuarios autenticados y no autenticados
3.9063			Los reportes debe mostrar marca de tiempo (Timestamp), Usuarios, Direcciones IP y nombres de dispositivos para usuarios autenticados y visitantes
3.9064			Soporte de Syslog y SNMP (Simple Network Management Protocol) para integración con otras soluciones de monitoreo
3.9065			Envío de alarmas sobre las métricas programadas cuando las políticas no se cumplen o no están aplicándose correctamente
3.9066			La solución debe contar con una arquitectura en capas que pueda operar en ambientes distribuidos (e.j. 2 ubicaciones distintas administradas desde un datacenter)

3.9067			Debe contar con diversos roles para una administración compartida con funciones limitadas para distintas áreas de la organización (e.j. administradores, solo lectura, reporteadores, etc.)
3.9068			Debe contar con información completa de los eventos de seguridad reportados para su investigación y troubleshooting de forma inmediata.
3.9069			Debe operar en un modo de aprendizaje al ser configurado a punto de acuerdo a las necesidades del negocio, con la finalidad de afinar las políticas y alertas antes de liberarse a producción
3.9070			La solución debe soportar todas las versiones vigentes de las familias de software Windows, Linux, Apple y Android
3.9071			Soporte completo con RSA - Secure ID
3.9072			Soporte Nativo de Microsoft Active Directory
3.9073			Soporte Nativo a Proxy/Servidor Radius
3.9074			Soporte Infraestructura de Comunicaciones de Terceros (Switches/Routers) - Telnet, SSL, SNMP
3.9075			Soporte de almacenamiento de logs - Integración con BITACORA
3.9076			Soporte a Checkpoint R65 a 75 - OPSEC - LEA
3.9077			Controladoras y Access Points Wireless LAN de Aruba, Cisco y Checkpoint
3.9078			Soporte Symantec Endpoint Protection
3.9079			Soporte Symantec DLP
3.9080			Soporte con SourceFire / McAfee IPS - Drop, TCP Reset, o similar
3.9081			Soporte a Linux / Unix - Cliente y Nativo

2.8.2 Condiciones Generales aplicables para todos los lotes de esta licitación

Condiciones Generales aplicables para todos los lotes de esta licitación	
Obligación de ofertar Soluciones completas, integradas y funcionales	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 incluyendo todos los elementos y servicios de integración entre ellas. 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 funcionalidad de la solución completa, en un formato llave en mano que incluya todos los elementos necesarios para su puesta en

	funcionamiento integral. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra. Este requerimiento no será sub-sanable.
Garantía, Soporte y Mantenimiento Técnico	Debe incluirse y describirse explícitamente la Garantía, el Soporte y Mantenimiento Técnico a todas las soluciones tanto de Hardware, incluyendo la sustitución de piezas, como de Licencias de Software, incluyendo actualización de los mismos, servicios de suscripción, y cualquier otro elemento necesario en cada una de las soluciones propuestas. Estos soportes deben ser por un tiempo de 3 años a partir de la puesta en marcha de la solución con un tiempo de respuesta de 4 horas y cobertura 7X24 para todas las soluciones requeridas, excepto para las soluciones de Seguridad Informática, para las mismas, el tiempo de respuesta requerido es de 2 horas y cobertura 7X24. Este soporte debe incluir tanto la Garantía del Fabricante por un período de 1 año, el soporte del oferente local, como el soporte oficial del fabricante de cada solución. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra. La propuesta económica debe incluir la Garantía del primer año, todos los servicios de soporte y mantenimiento técnico, actualización de software, suscripciones, para este primer año etc. Se debe incluir adicionalmente los precios de forma separada de estos servicios, soportes y mantenimientos para los años 2 y 3 de las soluciones. Estos años serán abonados por el Ministerio de Hacienda de acuerdo a las condiciones de pago referidas en el pliego. Este requerimiento no será sub-sanable.
Titular de las licencias de Software, Subscripciones , etc.	Todas las licencias de software, subscripciones, garantías, etc, deben ser ofertadas y emitidas a nombre del: "Ministerio de Hacienda, todas sus dependencias e instituciones descentralizadas". El Ministerio de Hacienda tendrá el derecho legal de usar las mismas bajo su única, absoluta y completa discreción dentro de cualquiera de sus dependencias oficiales sin que esto implique un cambio de titular de las licencias, subscripciones, etc, ni se incurra en ningún tipo de costo adicional por estos usos. Este requisito no será sub-sanable.
Referencia y Documentación de Requerimientos Técnicos	Las ofertas técnicas deben ser presentadas en el formulario de cumplimiento en un formato de manera tal que al lado de cada requerimiento técnico, en su línea correspondiente, se documente la referencia específica a la documentación técnica original de cada fabricante de los elementos propuestos donde se establece el cumplimiento o no de cada requerimiento. Los oferentes deberán presentar la documentación técnica original de cada fabricante para todas las soluciones y elementos ofertados.
Autorizaciones y Certificaciones de los fabricantes de todas las soluciones ofertadas	Los oferentes deberán proveer documentación original firmada y sellada en papel oficial de cada fabricante de las soluciones propuestas donde se establezca explicitamente que el proveedor está autorizado legalmente por el fabricante para ofertar las soluciones en

	territorio de la República Dominicana a entidades gubernamentales y en específico para esta licitación en particular y está Certificado y capacitado para ofrecer los servicios de instalación y soporte técnico de todas y cada una de las soluciones propuestas. Este requisito no será sub-sanable.
Gerente de Proyecto	Debe incluirse y describirse explícitamente la asignación de un gerente de proyectos certificado PMP dedicado 100% de su tiempo a la implantación de todas las soluciones ofertadas en este lote durante todo el tiempo que sea necesario y requerido por el Ministerio de Hacienda hasta la conclusión y recepción del proyecto. Se debe incluir en la propuesta el curriculum de este gerente de proyectos propuesto.
Project Plan	Debe incluirse y describirse explícitamente el Project Plan en formato de MS Project para la implementación de todas las soluciones ofertadas en este lote, así como los currículos del personal que sería asignado al mismo. El oferente que resulte ganador deberá mantener y actualizar este Project Plan con periodicidad semanal, y deberá justificar por escrito cualquier cambio que ocurriese con respecto al original.

2.8.3.1 Sistemas de Seguridad Lógica

Los Sistemas de Seguridad Lógica integrada para el Ministerio de Hacienda y dependencias deben cumplir los siguientes requisitos:

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 en este lote 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.
Todas las soluciones deben ser ofertadas en diseño operacional de alta disponibilidad	Todas las soluciones ofertadas en este lote deben incluir y describir explícitamente configuraciones con redundancia de alta disponibilidad en las mismas. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra.
Instalación, Configuración y	Deben incluirse y describirse explícitamente todos los servicios,

Puesta a Punto de las soluciones ofertadas	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.
Gerente de Proyecto	Debe incluirse y describirse explícitamente la asignación de un gerente de proyectos dedicado certificado PMP 100% de su tiempo a la implantación de todas las soluciones ofertadas en este lote durante todo el tiempo que sea necesario y requerido por el Ministerio de Hacienda. Se debe incluir en la propuesta el curriculum de este gerente de proyectos propuesto.
Project Plan	Debe incluirse y describirse explícitamente el Project Plan en formato de MS Project para la implantación de todas las soluciones ofertadas en este lote, así como los currículos del personal que sería asignado al mismo. El oferente que resulte ganador deberá mantener y actualizar este Project Plan con periodicidad semanal, y deberá justificar por escrito cualquier cambio que ocurriese con respecto al original.
Dimensionamiento General	Para los fines de dimensionamiento general pertinentes a cada solución propuesta, en caso de ser necesario, se deben licenciar 1400 usuarios locales, 1400 dispositivos, 500 Gbps de Tráfico de Internet y 400 máquinas de servidores virtuales para ambientes de aplicaciones. Este dimensionamiento tiene precedencia sobre cualquier error y/u omisión de las especificaciones de cada solución si se diese esa situación. Otros tipos de dimensionamientos particulares a cada solución se especifican en cada una de las mismas.
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. Este soporte debe ser por un tiempo de un (1) año 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. Este requerimiento tendrá precedencia sobre cualquier error u omisión en las descripciones particulares de cualquier solución en caso de que esto ocurra. Se debe incluir adicionalmente los precios de forma separada de estos servicios, soportes y mantenimientos para los años 2 y 3 de las soluciones. Estos años serán abonados por el Ministerio de Hacienda de acuerdo a las condiciones de pago referidas en el pliego. Este requerimiento no será sub-sanable.

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 ofrecerse en la Ciudad de Santo Domingo y deben incluir toda la documentación y material de soporte de los mismos. En caso de no poder ser ofrecidos en la Ciudad de Santo Domingo, se deben incluir los costos de viáticos para los mismos.

2.9 Duración del Suministro

La Convocatoria a Licitación se hace sobre la base de un suministro para un período de tres (3) años conforme se establezca en el Cronograma de Entrega de Cantidades Adjudicadas, si aplica.

2.10 Programa de Suministro

Los pedidos se librarán en el lugar designado por la Entidad Contratante en esta ciudad de Santo Domingo, República Dominicana (Incoterm DDP) y conforme al Cronograma de Entrega establecido.

2.11 Presentación de Propuestas Técnicas y Económicas "Sobre A" y "Sobre B"

Las Ofertas se presentarán en un Sobre cerrado y rotulado con las siguientes inscripciones:

NOMBRE DEL OFERENTE
(Sello social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
Ministerio de Hacienda
Referencia: MH-CCC-LPN- 2017-0010
Dirección: **Av. México No. 45, Gazcue**
Teléfono: **(809) 687–5131 ext. 2436**

Este Sobre contendrá en su interior el **"Sobre A"** Propuesta Técnica y el **"Sobre B"** Propuesta Económica.

Ninguna oferta presentada en término podrá ser desestimada en el acto de apertura. Las que fueren observadas durante el acto de apertura se agregaran para su análisis por parte de los peritos designados.

2.12 Lugar, Fecha y Hora

La presentación de Propuestas **"Sobre A" y "Sobre B"** se efectuará en acto público, ante el Comité de Compras y Contrataciones y el Notario Público actuante, **en el Salón Matías Ramón Mella, sito Av. México No.45, Gazcue, el día miércoles 06 de diciembre desde las 8:00 hasta las 09:30 A.M, Apertura sobre "A" 10:00 AM.**, y sólo podrá postergarse por causas de Fuerza Mayor o Caso Fortuito definidos en el presente Pliego de Condiciones Específicas.

La Entidad Contratante no recibirá sobres que no estuviesen debidamente cerrados e identificados según lo dispuesto anteriormente.

2.13 Forma para la Presentación de los Documentos Contenidos en el "Sobre A".

Los documentos contenidos en el "Sobre A" deberán ser presentados en original debidamente marcado como **DOS (2) "ORIGINALES** en la primera página del ejemplar, junto con UNA (1), fotocopia simple de los mismos, debidamente marcada, en su primera página, como "COPIA". Las originales y las copias deberán firmarse en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía. Adicional deben de enviar UNA (1) copia digital.

En adición a la presentación física de la Oferta Técnica del Sobre A, el Proponente deberá entregar una copia de la oferta en formato digital o magnético en archivo tipo PDF.

El "**Sobre A"** deberá contener en su cubierta la siguiente identificación:

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
Ministerio de Hacienda
PRESENTACIÓN: **OFERTA TÉCNICA**
REFERENCIA: MH-CCC-LPN- 2017-0010

2.14 Documentación a Presentar

A. Documentación Legal:
   1. Formulario de Presentación de Oferta.**(SNCCF.034)**
   2. Formulario de Información sobre Oferente.**(SNCCF.042)**
   3. Copia de los Estatutos Sociales del oferente participante, en caso de ser un oferente constituido bajo las leyes de la República Dominicana los indicados Estatutos deberán estar conforme a la Ley No. 479-08, de fecha 11 de diciembre de 2008, sobre las Sociedades Comerciales y Empresas Individuales de Responsabilidad Limitada y sus modificaciones;
   4. Copia legible, vigente y actualizada del Certificado de Registro Mercantil o equivalente del oferente, donde conste que se dedica(n) a la actividad comercial del ámbito de la licitación;
   5. Copia de la última Acta de Asamblea y Nómina de Presencia del oferente;
   6. Constancia de inscripción en el Registro de Proveedores del Estado (RPE) en donde el oferente acredite su inscripción en un rubro de la actividad comercial requerida para participar en esta licitación. En el caso de un oferente extranjero, no necesitará estar registrado en el RPE, salvo el caso de que se encuentre domiciliado en la República Dominicana. Sin embargo, si resulta adjudicatario, previa suscripción del contrato, deberá obtener y depositar el registro correspondiente, según lo establecido en los artículos del 21 al 25 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, sobre el Reglamento de aplicación de la precitada Ley No. 340-06.

7.
8. El Registro de Proveedores del Estado (RPE) deberá estar actualizado conforme lo establece el artículo 19 del Decreto No. 543-12, de fecha 6 de septiembre de 2012, sobre el Reglamento de aplicación de la Ley No. 340-06 y sus modificaciones, así como la Resolución No. 14-2015, de fecha 27 de enero de 2015, dictada por la Dirección General de Contrataciones Públicas;
9. El oferente nacional o extranjero, aún se encuentre inscrito en el Registro de Proveedores del Estado (RPE), deberá presentar una (1) declaración simple en original, en las que se haga constar lo siguiente:

Que el oferente no se encuentra afectado por las prohibiciones establecidas en el artículo 14 de la Ley No. 340-06 y sus modificaciones, sobre Compras y Contrataciones de Bienes, Servicios, Obras y Concesiones.

Que el oferente tiene o no juicios 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.

10. El oferente deberá utilizar el modelo de declaración simple que dispone la Dirección General de Contrataciones Públicas, para estos fines;
11. Certificación actualizada y legible de la Dirección General de Impuestos Internos (DGII) o en su defecto del organismo que en el país de origen del Oferente (si éste no se encuentra domiciliado y/o legalmente representado en la República Dominicana) sea el que determine que se encuentra al día en el pago de sus obligaciones fiscales;
12. Certificación de pago de la Tesorería de la Seguridad Social (TSS) del oferente. En el caso de un oferente extranjero, este requisito sólo aplicará cuando dicho oferente se encuentre domiciliado y/o legalmente representado en la República Dominicana;
13. Poder de Representación otorgado ante Notario Público Nacional o copia del Acta de la Asamblea del Consejo de Administración o de la Asamblea General de Accionistas u Socios, según sea el caso. Si la sociedad comercial participante está representada por su Presidente o Gerente, y siempre y cuando los Estatutos Sociales le otorguen el Poder de Representación de la sociedad, no es necesario presentar este requerimiento;
14. Copia legible y vigente de la Cédula de Identidad y Electoral del Representante Legal. En caso de ser extranjero con residencia, depositará copia legible y vigente de la Cédula de Identidad o Pasaporte si no reside en el país.

B. Documentación Financiera:
   1. Estados Financieros de los **dos (2)** últimos ejercicios contables consecutivos.

C. Documentación Técnica:
   1. Oferta Técnica (conforme a las especificaciones técnicas suministradas);
   2. Autorización del Fabricante para la venta, instalación y soporte tanto para la Republica Dominicana como para esta licitación en específico, en los casos de que los Bienes no sean fabricados por el Oferente **(SNCC.F.047)**;
   3. Brochures originales de los fabricantes de los equipos a ser suministrados;

4. Al lado de cada especificación técnica de la tabla de cumplimiento se debe indicar la página de cada brochure donde se avale dicho requerimiento;
5. Deberán entregar toda la documentación solicitada en las especificaciones técnicas anexas en este Pliego de Condiciones.

Para los consorcios:

En adición a los requisitos anteriormente expuestos, los consorcios deberán presentar:

1. Original del Acto Notarial por el cual se formaliza el consorcio, incluyendo su objeto, las obligaciones de las partes, su duración la capacidad de ejercicio de cada miembro del consorcio, así como sus generales; y
2. Poder especial de designación del representante o gerente único del Consorcio autorizado por todas las empresas participantes en el consorcio.

2.16 Presentación de la Documentación Contenida en el "Sobre B"

A) Formulario de Presentación de Oferta Económica (SNCC.F.33), presentado en **Dos (2)** originales debidamente marcados como "**ORIGINALES**" en la primera página de la Oferta, junto con **una (1)** fotocopia simple de la misma, debidamente marcada, en su primera página, como "**COPIA**" Y **una (1)** versión digital. El original y las copias deberán estar firmados en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía.

B) Garantía de la Seriedad de la Oferta. Correspondiente a **Póliza de Fianza o Garantía Bancaria.** La vigencia de la garantía deberá ser igual al plazo de validez de la oferta establecido en el numeral 3.8 del presente Pliego de Condiciones.

Se deberán presentar las propuestas económicas con tres (3) montos separados: el primer monto deberá incluir el costo de adquisición de los Bienes y Servicios y el primer año de soporte técnico de los mismos. El segundo y tercer monto deben corresponder a los soportes técnicos de los años subsiguientes.

''Para los fines de la evaluación económica de las propuestas el monto a considerar será la suma de los tres (3) montos requeridos.''

El **"Sobre B"** deberá contener en su cubierta la siguiente identificación:

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
Ministerio de Hacienda
PRESENTACIÓN: **OFERTA ECONÓMICA**
REFERENCIA: MH-CCC-LPN- 2017-0010

Las Ofertas deberán ser presentadas únicas y exclusivamente en el formulario designado al efecto, **(SNCC.F.033)**, **siendo inválida toda oferta bajo otra presentación**.

La Oferta Económica deberá presentarse en Pesos Dominicanos (RD$). Los precios deberán expresarse en **dos decimales (XX.XX)** que tendrán que incluir todas las tasas (divisas), impuestos y gastos que correspondan, transparentados e implícitos según corresponda.

El Oferente será responsable y pagará todos los impuestos, derechos de aduana, o gravámenes que hubiesen sido fijados por autoridades municipales, estatales o gubernamentales, dentro y fuera de la República Dominicana, relacionados con los bienes y servicios conexos a ser suministrados.
Ninguna institución sujeta a las disposiciones de la Ley que realice contrataciones, podrá contratar o convenir sobre disposiciones o cláusulas que dispongan sobre exenciones o exoneraciones de impuestos y otros atributos, o dejar de pagarlos, sin la debida aprobación del Congreso Nacional.

El Oferente/Proponente que cotice en cualquier moneda distinta al Peso Dominicano (RD$), **se auto-descalifica para ser adjudicatario.**

A fin de cubrir las eventuales variaciones de la tasa de cambio del Dólar de los Estados Unidos de Norteamérica (US$), **Ministerio de Hacienda** podrá considerar eventuales ajustes, una vez que las variaciones registradas sobrepasen el **cinco por ciento (5%)** con relación al precio adjudicado o de última aplicación. La aplicación del ajuste podrá ser igual o menor que los cambios registrados en la Tasa de Cambio Oficial del Dólar Americano (US$) publicada por el Banco Central de la República Dominicana, a la fecha de la entrega de la Oferta Económica.

En el caso de que el Oferente/Proponente Adjudicatario solicitara un eventual ajuste, **Ministerio de Hacienda** se compromete a dar respuesta dentro de los siguientes **cinco (5) días laborables**, contados a partir de la fecha de acuse de recibo de la solicitud realizada.

La solicitud de ajuste no modifica el Cronograma de Entrega de Cantidades Adjudicadas, por lo que, el Proveedor Adjudicatario se compromete a no alterar la fecha de programación de entrega de los Bienes pactados, bajo el alegato de esperar respuesta a su solicitud.

Los precios no deberán presentar alteraciones ni correcciones y **deberán ser dados en la unidad de medida establecida en el Formulario de Oferta Económica.**

En los casos en que la Oferta la constituyan varios bienes, solo se tomará en cuenta la cotización únicamente de lo evaluado CONFORME en el proceso de evaluación técnica.

Será responsabilidad del Oferente/Proponente la adecuación de los precios unitarios a las unidades de medidas solicitadas, considerando a los efectos de adjudicación el precio consignado en la Oferta Económica como el unitario y valorándolo como tal, respecto de otras Ofertas de los mismos productos. El Comité de Compras y Contrataciones, no realizará ninguna conversión de precios unitarios si éstos se consignaren en unidades diferentes a las solicitadas.

Sección III
Apertura y Validación de Ofertas

3.1 Procedimiento de Apertura de Sobres

La apertura de Sobres se realizará en acto público en presencia del Comité de Compras y Contrataciones y del Notario Público actuante, en la fecha, lugar y hora establecidos en el Cronograma de Licitación.

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.

3.2 Apertura de "Sobre A", contentivo de Propuestas Técnicas

El Notario Público actuante procederá a la apertura de los "**Sobres A"**, según el orden de llegada, procediendo a verificar que la documentación contenida en los mismos esté correcta de conformidad con el listado que al efecto le será entregado. El Notario Público actuante, deberá rubricar y sellar cada una de las páginas de los documentos contenidos en los "**Sobres A"**, haciendo constar en el mismo la cantidad de páginas existentes.

En caso de que surja alguna discrepancia entre la relación y los documentos efectivamente presentados, el Notario Público autorizado dejará constancia de ello en el acta notarial.

El Notario Público actuante elaborará el acta notarial correspondiente, incluyendo las observaciones realizadas en el desarrollo del acto de apertura de los Sobres A, si las hubiere.

El Notario Público actuante concluido el acto de recepción, dará por cerrado el mismo, indicando la hora de cierre.

Las actas notariales estarán disponibles para los Oferentes/ Proponentes, o sus Representantes Legales, quienes para obtenerlas deberán hacer llegar su solicitud a través de la Oficina de Acceso a la Información (OAI).

3.3 Validación y Verificación de Documentos

Los Peritos, procederá a la validación y verificación de los documentos contenidos en el referido "**Sobre A".** Ante cualquier duda sobre la información presentada, podrá comprobar, por los medios que considere adecuados, la veracidad de la información recibida.

No se considerarán aclaraciones a una Oferta presentadas por Oferentes cuando no sean en respuesta a una solicitud de la Entidad Contratante. La solicitud de aclaración por la Entidad Contratante y la respuesta deberán ser hechas por escrito.

Antes de proceder a la evaluación detallada del "**Sobre A",** los Peritos determinarán si cada Oferta se ajusta sustancialmente al presente Pliego de Condiciones Específica; o si existen desviaciones, reservas, omisiones o errores de naturaleza o de tipo subsanables de conformidad a lo establecido en el numeral 1.21 del presente documento.

En los casos en que se presenten desviaciones, reservas, omisiones o errores de naturaleza o tipo subsanables, los Peritos Especialistas procederán de conformidad con los procedimientos establecidos en el presente Pliego de Condiciones Específicas.

3.4 Criterios 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, ofertar los servicios de instalación y de soporte técnico en el país.

Capacidad Técnica

1. Que el Proponente demuestre capacidad técnica y que los Bienes y Servicios cumplen con todas características especificadas en las descripciones de las Fichas Técnicas; y

2. Se evaluarán las propuestas técnicas de cada oferente, si en alguna de las líneas de especificaciones técnicas, la propuesta de algún oferente no cumple, se determinará que la propuesta completa no cumple.

Situación financiera

Que cuenta con la estabilidad financiera suficiente para ejecutar satisfactoriamente el eventual Contrato.

El Oferente deberá presentar los Estados Financieros de los dos (2) últimos ejercicios contables consecutivos. Obligatoriamente estarán firmados por un Contador Público Autorizado, siendo causal de exclusión la no presentación de alguno de los mismos o la falta de certificación.

Sobre el último balance, se aplicarán para su análisis los siguientes indicadores:

a) Índice de solvencia = ACTIVO TOTAL / PASIVO TOTAL
Límite establecido: Mayor 1.20

b) Índice de liquidez corriente = ACTIVO CORRIENTE / PASIVO CORRIENTE
Límite establecido: Mayor 0.9

c) Índice de endeudamiento = PASIVO TOTAL/ PATRIMONIO NETO
Límite establecido: Menor 1.50

Criterios particulares

La evaluación de las propuestas será en base a lotes individuales, por lo que al lado de cada especificación técnica de la tabla de cumplimiento, se verificará en la página de cada brochure donde los Oferentes avalaron dicho requerimiento.

Para los fines de la evaluación económica de las propuestas el monto a considerar será la suma de los tres (3) montos requeridos.

3.5 Fase de Homologación

Para que un Bien pueda ser considerado **CONFORME**, deberá cumplir con todas y cada una de las características contenidas en las referidas Fichas Técnicas. Es decir que, el no cumplimiento en una de las especificaciones, implica la descalificación de la Oferta y la declaración de **NO CONFORME** del Bien ofertado.

Los Peritos levantarán un informe donde se indicará el cumplimiento o no de las Especificaciones Técnicas de cada uno de los Bienes ofertados, bajo el criterio de **CONFORME/ NO CONFORME**. 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.

3.6 Apertura de los "Sobres B", Contentivos de Propuestas Económicas

El Comité de Compras y Contrataciones, dará inicio al Acto de Apertura y lectura de las Ofertas Económicas, **"Sobre B",** conforme a la hora y en el lugar indicado.

Sólo se abrirán las Ofertas Económicas de los Oferentes/Proponentes que hayan resultado habilitados en la primera etapa del proceso. Son éstos aquellos que una vez finalizada la evaluación de las Ofertas Técnicas, cumplan con los criterios señalados en la sección Criterios de evaluación. Las demás serán devueltas sin abrir. De igual modo, solo se dará lectura a los renglones que hayan resultado CONFORME en el proceso de evaluación de las Ofertas Técnicas.

A la hora fijada en el Cronograma de la Licitación, el Consultor Jurídico de la institución, en su calidad de Asesor Legal del Comité de Compras y Contrataciones, hará entrega formal al Notario Público actuante, en presencia de los Oferentes, de las Propuestas Económicas, **"Sobre B",** que se mantenían bajo su custodia, para dar inicio al procedimiento de apertura y lectura de las mismas.

En acto público y en presencia de todos los interesados el Notario actuante procederá a la apertura y lectura de las Ofertas Económicas, certificando su contenido, rubricando y sellando cada página contenida en el **"Sobre B".**

Las observaciones referentes a la Oferta que se esté leyendo, deberán realizarse en ese mismo instante, levantando la mano para tomar la palabra. El o los Notarios actuantes procederán a hacer constar todas las incidencias que se vayan presentando durante la lectura.

Finalizada la lectura de las Ofertas, el o los Notarios actuantes procederán a invitar a los Representantes Legales de los Oferentes/Proponentes a hacer conocer sus observaciones; en caso de conformidad, se procederá a la clausura del acto.

No se permitirá a ninguno de los presentes exteriorizar opiniones de tipo personal o calificativos peyorativos en contra de cualquiera de los Oferentes participantes.

El Oferente/Proponente o su representante que durante el proceso de la Licitación tome la palabra sin ser autorizado o exteriorice opiniones despectivas sobre algún producto o compañía, será sancionado con el retiro de su presencia del salón, con la finalidad de mantener el orden.

En caso de discrepancia entre la Oferta presentada en el formulario correspondiente, **(SNCC.F.033)**, debidamente recibido por el Notario Público actuante y la lectura de la misma, prevalecerá el documento escrito.

El o los Notarios Públicos actuantes elaborarán el acta notarial correspondiente, incluyendo las observaciones realizadas al desarrollo del acto de apertura, si las hubiera, por parte de los Representantes Legales de los Oferentes/ Proponentes. El acta notarial deberá estar acompañada de una fotocopia de todas las Ofertas presentadas. Dichas actas notariales estarán disponibles para los Representantes Legales de los Oferentes/Proponentes, quienes para obtenerlas deberán hacer llegar su solicitud a través de la Oficina de Acceso a la Información (OAI).

3.7 Confidencialidad del Proceso

Las informaciones relativas al análisis, aclaración, evaluación y comparación de las Ofertas y las recomendaciones para la Adjudicación del Contrato no podrán ser reveladas a los Licitantes ni a otra persona que no participe oficialmente en dicho proceso hasta que se haya anunciado el nombre del Adjudicatario, a excepción de que se trate del informe de evaluación del propio Licitante. Todo intento de un Oferente para influir en el procesamiento de las Ofertas o decisión de la Adjudicación por parte del Contratante podrá dar lugar al rechazo de la Oferta de ese Oferente.

3.8 Plazo de Mantenimiento de Oferta

Los Oferentes/Proponentes deberán mantener las Ofertas por el término de **noventa (90)** días hábiles contados a partir de la fecha del acto de apertura.

La Entidad Contratante, excepcionalmente podrá solicitar a los Oferentes/Proponentes una prórroga, antes del vencimiento del período de validez de sus Ofertas, con indicación del plazo. Los Oferentes/Proponentes podrán rechazar dicha solicitud, considerándose por tanto que han retirado sus Ofertas, por lo cual la Entidad Contratante procederá a efectuar la devolución de la Garantía de Seriedad de Oferta ya constituida. Aquellos que la consientan no podrán modificar sus Ofertas y deberán ampliar el plazo de la Garantía de Seriedad de Oferta oportunamente constituida.

3.9 Evaluación Oferta Económica

El Comité de Compras y Contrataciones evaluará y comparará 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 menor precio ofertado.

Sección IV
Adjudicación

4.1 Criterios de Adjudicación

El Comité de Compras y Contrataciones evaluará las Ofertas dando cumplimiento a los principios de transparencia, objetividad, economía, celeridad y demás, que regulan la actividad contractual, y comunicará por escrito al Oferente/Proponente que resulte favorecido. Al efecto, se tendrán en cuenta los factores económicos y técnicos más favorables.

La Adjudicación será decidida a favor del Oferente/Proponente cuya propuesta cumpla con los requisitos exigidos y sea calificada como la más conveniente para los intereses institucionales, teniendo en cuenta el precio, la calidad, y las demás condiciones que se establecen en el presente Pliego de Condiciones Específicas.

Si se presentase una sola Oferta, ella deberá ser considerada y se procederá a la Adjudicación, si habiendo cumplido con lo exigido en el Pliego de Condiciones Específicas, se le considera conveniente a los intereses de la Institución.

4.2 Empate entre Oferentes

En caso de empate entre dos o más Oferentes/Proponentes, se procederá de acuerdo al siguiente procedimiento:

El Comité de Compras y Contrataciones procederá por una elección al azar, en presencia de Notario Público y de los interesados, utilizando para tales fines el procedimiento de sorteo.

4.3 Declaración de Desierto

El Comité de Compras y Contrataciones podrá declarar desierto el procedimiento, total o parcialmente, en los siguientes casos:

- Por no haberse presentado Ofertas.
- Por haberse rechazado, descalificado, o porque son inconvenientes para los intereses nacionales o institucionales todas las Ofertas o la única presentada.

En la Declaratoria de Desierto, la Entidad Contratante podrá reabrirlo dando un plazo para la presentación de Propuestas de hasta un **cincuenta por ciento (50%)** del plazo del proceso fallido.

4.4 Acuerdo de Adjudicación

El Comité de Compras y Contrataciones luego del proceso de verificación y validación del informe de recomendación de Adjudicación, conoce las incidencias y si procede, aprueban el mismo y emiten el acta contentiva de la Resolución de Adjudicación.

Ordena a la Unidad Operativa de Compras y Contrataciones la Notificación de la Adjudicación y sus anexos a todos los Oferentes participantes, conforme al procedimiento y plazo establecido en el Cronograma de Actividades del Pliego de Condiciones Específicas.

4.5 Adjudicaciones Posteriores

En caso de incumplimiento del Oferente Adjudicatario, la Entidad Contratante procederá a solicitar, mediante ***"Carta de Solicitud de Disponibilidad"***, al siguiente Oferente/Proponente que certifique si está en capacidad de suplir los renglones que le fueren indicados. Dicho Oferente/Proponente contará con un plazo de **Cuarenta y Ocho (48) horas** para responder la referida solicitud. En caso de respuesta afirmativa, El Oferente/Proponente deberá presentar la Garantía de Fiel cumplimiento de Contrato, conforme se establece en los **DDL.**

PARTE 2
CONTRATO

Sección V
Disposiciones Sobre los Contratos

5.1 Condiciones Generales del Contrato

5.1.1 Validez del Contrato

El Contrato será válido cuando se realice conforme al ordenamiento jurídico y cuando el acto definitivo de Adjudicación y la constitución de la Garantía de Fiel Cumplimiento de Contrato sean cumplidos.

5.1.2 Garantía de Fiel Cumplimiento de Contrato

La Garantía de Fiel Cumplimiento de Contrato corresponderá a una Garantía Bancaria, la vigencia de ésta deberá cubrir el período de contrato, que será por tres (3) años.

5.1.3 Perfeccionamiento del Contrato

Para su perfeccionamiento deberán seguirse los procedimientos de contrataciones vigentes, cumpliendo con todas y cada una de sus disposiciones y el mismo deberá ajustarse al modelo que se adjunte al presente Pliego de Condiciones Específicas, conforme al modelo estándar el Sistema Nacional de Compras y Contrataciones Públicas.

5.1.4 Plazo para la Suscripción del Contrato

Los Contratos deberán celebrarse en el plazo que se indique en el presente Pliego de Condiciones Específicas; no obstante a ello, deberán suscribirse en un plazo no mayor de **veinte (20) días hábiles**, contados a partir de la fecha de Notificación de la Adjudicación.

5.1.5 Incumplimiento del Contrato

Se considerará incumplimiento del Contrato:

a. La mora del Proveedor en la entrega de los Bienes.

b. La falta de calidad de los Bienes suministrados.

c. El Suministro de menos unidades de las solicitadas, no aceptándose partidas incompletas para los adjudicatarios en primer lugar.

d. Incumplimiento de los plazos de ejecución presentados en el Plan de Proyecto requerido.

5.1.6 Efectos del Incumplimiento

El incumplimiento del Contrato por parte del Proveedor determinará su finalización y supondrá para el mismo la ejecución de la Garantía Bancaria de Fiel Cumplimiento del Contrato, procediéndose a contratar al Adjudicatario que haya quedado en el 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, la Entidad Contratante podrá solicitar a la Dirección General de Contrataciones Pública, en su calidad de Órgano Rector del Sistema, su inhabilitación temporal o definitiva, dependiendo de la gravedad de la falta.

5.1.7 Ampliación o Reducción de la Contratación

La Entidad Contratante no podrá producir modificación alguna de las cantidades previstas en el Pliego de Condiciones Específicas.

5.1.8 Finalización del Contrato

El Contrato finalizará por vencimiento de su plazo, o por la concurrencia de alguna de las siguientes causas de resolución:

- Incumplimiento del Proveedor.
- Incursión sobrevenida del Proveedor en alguna de las causas de prohibición de contratar con la Administración Pública que establezcan las normas vigentes, en especial el Artículo 14 de la Ley No. 340-06, sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones.

5.1.9 Subcontratos

En ningún caso el Proveedor podrá ceder los derechos y obligaciones del Contrato a favor de un tercero, ni tampoco estará facultado para subcontratarlos sin la autorización previa y por escrito de la Entidad Contratante.

5.2 Condiciones Específicas del Contrato

5.2.1 Condiciones Generales aplicables.

Las Condiciones Generales aplicables del presente procedimiento, se aplicarán en el contrato a suscribir con el adjudicatario, dentro de las que se encuentran:

-Garantía, Soportes y Mantenimiento Técnico;
-Titularidad de las licencias de software, subscripción, etc. a nombre del Ministerio de Hacienda y sus dependencias;
-Autorizaciones y certificaciones de los fabricantes de todas las soluciones ofertas;
-Documentación a presentar;
-Tener un Gerente de proyecto;
-Disponer de Project Plan; e
-Integrar los Sistemas de Seguridad Lógica.

5.2.2 Vigencia del Contrato

La vigencia del Contrato será de tres (3) años, a partir de la fecha de la suscripción de éste y hasta su fiel cumplimiento, de conformidad con el Cronograma de Entrega de Cantidades Adjudicadas, el cual formará parte integral y vinculante del mismo.

5.2.3 Inicio del Suministro

Una vez formalizado el correspondiente Contrato de Suministro entre la Entidad Contratante y el Proveedor, éste último iniciará el Suministro de los Bienes que se requieran mediante el correspondiente pedido, sustentado en el Cronograma de Entrega de Cantidades Adjudicadas, que forma parte constitutiva, obligatoria y vinculante del presente Pliego de Condiciones Específicas.

5.2.4 Modificación del Cronograma de Entrega

La Entidad Contratante, como órgano de ejecución del Contrato tendrá el derecho de modificar el Cronograma de Entrega de los Bienes Adjudicados, conforme entienda oportuno a los intereses de la institución.

Si el Proveedor no suple los Bienes en el plazo requerido, se entenderá que el mismo renuncia a su Adjudicación y se procederá a declarar como Adjudicatario al que hubiese obtenido el segundo (2do.) lugar y así sucesivamente, en el orden de Adjudicación y de conformidad con el Reporte de Lugares Ocupados. De presentarse esta situación, la Entidad Contratante procederá a ejecutar la Garantía Bancaria de Fiel Cumplimiento del Contrato, como justa indemnización por los daños ocasionados.

5.2.5 Entregas Subsiguientes

Las entregas subsiguientes se harán de conformidad con el Cronograma de Entrega establecido.

Las Adjudicaciones a lugares posteriores podrán ser proporcionales, y el Adjudicatario deberá indicar su disponibilidad en un plazo de **Cuarenta y Ocho (48) horas**, contadas a partir de la recepción de la Carta de Solicitud de Disponibilidad que al efecto le será enviada.

Los documentos de despacho a los almacenes de la Entidad Contratante deberán reportarse según las especificaciones consignadas en la Orden de Compra, la cual deberá estar acorde con el Pliego de Condiciones Específicas.

PARTE 3
ENTREGA Y RECEPCIÓN

Sección VI
Recepción de los Productos

6.1 Requisitos de Entrega

Todos los bienes, obras y servicios adjudicados deben ser entregados conforme a las especificaciones técnicas solicitadas, así como en el lugar de entrega convenido con **el Ministerio de Hacienda**, siempre con previa coordinación con el responsable de recibir la mercancía y con el encargado del almacén con fines de dar entrada a los bienes entregados.

6.2 Recepción Provisional

El Encargado de Almacén y Suministro debe recibir los bienes de manera provisional hasta tanto verifique que los mismos corresponden con las características técnicas de los bienes adjudicados.

6.3 Recepción Definitiva

Si los Bienes son recibidos CONFORME y de acuerdo a lo establecido en el presente Pliegos de Condiciones Específicas, en el Contrato u Orden de Compra, se procede a la recepción definitiva y a la entrada en Almacén para fines de inventario.

No se entenderán suministrados, ni entregados los Bienes que no hayan sido objeto de recepción definitiva.

6.4 Obligaciones del Proveedor

El Proveedor está obligado a reponer Bienes deteriorados durante su transporte o en cualquier otro momento, por cualquier causa que no sea imputable a la Entidad Contratante.

Si se estimase que los citados Bienes no son aptos para la finalidad para la cual se adquirieron, se rechazarán los mismos y se dejarán a cuenta del Proveedor, quedando la Entidad Contratante exenta de la obligación de pago y de cualquier otra obligación.

El Proveedor es el único responsable ante Entidad Contratante de cumplir con el Suministro de los renglones que les sean adjudicados, en las condiciones establecidas en los presente Pliegos de Condiciones Específicas. El Proveedor responderá de todos los daños y perjuicios causados a la Entidad Contratante y/o entidades destinatarias y/o frente a terceros derivados del proceso contractual.

Sección VII
Formularios

7.1 Formularios Tipo

El Oferente/Proponente deberá presentar sus Ofertas de conformidad con los Formularios determinados en el presente Pliego de Condiciones Específicas**, los cuales se anexan como parte integral del mismo.**

7.2 Anexos

1. Modelo de Contrato de Suministro de Bienes **(SNCC.C.023)**
2. Formulario de Oferta Económica **(SNCC.F.033)**
3. Presentación de Oferta **(SNCC.F.034)**
4. Garantía bancaria de Fiel Cumplimiento de Contrato **(SNCC.D.038)**, si procede.
5. Formulario de Información sobre el Oferente **(SNCC.F.042)**
6. Formulario de Autorización del Fabricante **(SNCC.F.047)**, si procede.