REPÚBLICA DOMINICANA

SUPERINTENDENCIA DE BANCOS
DE LA REPÚBLICA DOMINICANA

TERMINOS DE REFERENCIA PARA LA ADQUISICION Y CONTRATACION DE BIENES Y SERVICIOS DE TECNOLOGIA PARA LA SUPERINTENDENCIA DE BANCOS

LICITACION PÚBLICA No. SIB-LPN-002/2019

Santo Domingo, Distrito Nacional
República Dominicana
25 de Noviembre 2019

TABLA DE CONTENIDO

GENERALIDADES 5

Prefacio 5

PARTE I 8

PROCEDIMIENTOS DE LA LICITACIÓN 8

Sección I 8

Instrucciones a los Oferentes (IAO) 8

1.1 Objetivos y Alcance 8
1.2 Definiciones e Interpretaciones 8
1.3 Idioma 12
1.4 Precio de la Oferta 12
1.5 Moneda de la Oferta 12
1.6 Normativa Aplicable 12
1.7 Competencia Judicial 13
1.8 Proceso Arbitral 13
1.9 De la Publicidad 13
1.10 Etapas de la Licitación 14
1.11 Órgano de Contratación 14
1.12 Atribuciones 14
1.13 Órgano Responsable del Proceso 14
1.14 Exención de Responsabilidades 15
1.15 Prácticas Corruptas o Fraudulentas 15
1.16 De los Oferentes/ Proponentes Hábiles e Inhábiles 15
1.17 Prohibición a Contratar 15
1.18 Demostración de Capacidad para Contratar 17
1.19 Representante Legal 18
1.20 Subsanaciones 18
1.21 Rectificaciones Aritméticas 18
1.22 Garantías 19
1.23.1 Garantía de la Seriedad de la Oferta 19
1.23.2 Garantía de Fiel Cumplimiento de Contrato 19
1.23 Devolución de las Garantías 20
1.24 Consultas 20
1.25 Circulares 20
1.26 Enmiendas 20
1.27 Reclamos, Impugnaciones y Controversias 21

Sección II 22

Datos de la Licitación (DDL) 22

2.1 Objeto de la Licitación 22
2.2 Procedimiento de Selección 22
2.3 Fuente de Recursos 22
2.4 Condiciones de Pago 22
2.5 Cronograma de la Licitación 23
2.6 Disponibilidad y Adquisición del Pliego de Condiciones 23
2.7 Conocimiento y Aceptación del Pliego de Condiciones 24
2.8 Descripción de los Bienes 24
2.9 Duración del Suministro 70

2.10 Programa de Suministro 70
2.11 Presentación de Propuestas Técnicas y Económicas "Sobre A" y "Sobre B" 70
2.12 Lugar, Fecha y Hora 71
2.13 Forma para la Presentación de los Documentos Contenidos en el "Sobre A", y Muestras 71
2.14 Documentación a Presentar 72
2.15 Forma de Presentación de las Muestras de los Productos 73
2.16 Presentación de la Documentación Contenida en el "Sobre B" 73

Sección III 75

Apertura y Validación de Ofertas 75
3.1 Procedimiento de Apertura de Sobres 75
3.2 Apertura de "Sobre A", contentivo de Propuestas Técnicas 76
3.3 Validación y Verificación de Documentos 76
3.4 Criterios de Evaluación 76
3.5 Fase de Homologación 77
3.6 Apertura de los "Sobres B", Contentivos de Propuestas Económicas 77
3.7 Confidencialidad del Proceso 78
3.8 Plazo de Mantenimiento de Oferta 78
3.9 Evaluación Oferta Económica 79

Sección IV 79

Adjudicación 79
4.1 Criterios de Adjudicación 79
4.2 Empate entre Oferentes 79
4.3 Declaración de Desierto 79
4.4 Acuerdo de Adjudicación 80
4.5 Adjudicaciones Posteriores 80

PARTE 2 80

CONTRATO 80

Sección V 80

Disposiciones Sobre los Contratos 80
5.1 Condiciones Generales del Contrato 80
5.1.1 Validez del Contrato 80
5.1.2 Garantía de Fiel Cumplimiento de Contrato 80
5.1.3 Perfeccionamiento del Contrato 80
5.1.4 Plazo para la Suscripción del Contrato 81
5.1.5 Incumplimiento del Contrato 81
5.1.6 Efectos del Incumplimiento 81
5.1.7 Ampliación o Reducción de la Contratación 81
5.1.8 Finalización del Contrato 81
5.1.9 Subcontratos 82
5.2 Condiciones Específicas del Contrato 82
5.2.1 Vigencia del Contrato 82
5.2.2 Inicio del Suministro 82
5.2.3 Modificación del Cronograma de Entrega 83
5.2.4 Entregas Subsiguientes 83

PARTE 3 83

ENTREGA Y RECEPCIÓN 83

Sección VI 83

Recepción de los Productos 83

6.1 Requisitos de Entrega 83
6.2 Recepción Provisional 83
6.3 Recepción Definitiva 84
6.4 Obligaciones del Proveedor 84

Sección VII..... 84

Formularios 84
7.1 Formularios Tipo 84

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 RECEPCION

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 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 Licitación para la **Adquisición y Contratación de Bienes y Servicios de Tecnología,** llevada a cabo por **Superintendencia de Bancos de la Republica Dominicana,** la cual tiene por referencia **SIB-LPN-002/2019.**

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.

1.2 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 oferentes(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.

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.

1.3 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.

1.4 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.

Todos los lotes 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 lote o 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).**

1.5 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.

1.6 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.

1.7 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.

1.8 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).

1.9 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 **treinta (30) 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.

1.10 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.

1.11 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.

1.12 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.

1.13 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.

1.14 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.

1.15 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.

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.

1.16 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.

1.17 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;

PARRAFO 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.

PARRAFO 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.

1.18 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;

1.19 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.

1.20 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.

1.21 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.

1.22 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.

1.23 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.

1.24 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
Superintendencia de Bancos de la República Dominicana
Referencia: SIB-LPN-002/2019
Dirección: Av. México #52, Esq. Leopoldo Navarro, Gazcue, Santo Domingo, R.D.
Teléfonos: 809-685-8141 ext. 276
Fax: 809-686-2874
Correo: wsolis@sib.gob.do

1.25 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.

1.26 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.

1.27 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.

Sección II
Datos de la Licitación (DDL)

2.1 Objeto de la Licitación

Constituye el objeto de la presente convocatoria la **Adquisición y Contratación de Bienes y Servicios de Tecnología** de acuerdo con las condiciones fijadas en el presente Pliego de Condiciones Específicas.

2.2 Procedimiento de Selección

Etapa Única

2.3 Fuente de Recursos

La Superintendencia de Bancos de la República Dominicana, 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 del Presupuesto del año **2019,** que sustentará 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 no podrá comprometerse a entregar, por concepto de avance, un porcentaje mayor al veinte por ciento (20%) del valor del Contrato.

En caso de que el adjudicatario del contrato sea una Micro, Pequeña y Mediana empresa (MIPYME) la entidad contratante deberá entregar un avance inicial correspondiente al veinte por ciento (20%) del

valor del contrato, para fortalecer su capacidad económica, contra la presentación de la garantía del buen uso del anticipo.

2.5 Cronograma de la Licitación

ACTIVIDADES	PERÍODO DE EJECUCIÓN
1. Publicación llamado a participar en la licitación	Lunes 25 y Martes 26 de Noviembre 2019
2. Período para realizar consultas por parte de los interesados	Martes 17 de Diciembre 2019
3. Plazo para emitir respuesta por parte del Comité de Compras y Contrataciones	Viernes 27 de Diciembre 2019
4. Recepción de Propuestas y Apertura de: "Sobre A" y "Sobre B"	**Viernes 10 de Enero 2020 Desde las 10:00 am en el Salón de Multiusos de la SIB**
5. Verificación, Validación y Evaluación contenido de las Propuestas Técnicas "Sobre A" y Homologación de Muestras.	Del lunes 13 al viernes 17 de Enero 2020
6. Notificación de errores u omisiones de naturaleza subsanables.	Viernes 17 de Enero 2020
7. Periodo de subsanación de ofertas	Del viernes 17 al miércoles 22 de enero 2020
8. Período de Ponderación de Subsanaciones	Del miércoles 22 al viernes 24 de Enero 2020
9. Evaluación Final de las Ofertas	Del viernes 24 al viernes 31 de Enero 2020
10. Adjudicación	Martes 4 de Febrero 2020
11. Notificación y Publicación de Adjudicación	Martes 11 de Febrero 2020
12. Plazo para la constitución de la Garantía Bancaria de Fiel Cumplimiento de Contrato	Martes 18 de Febrero 2020
13. Suscripción del Contrato	Martes 10 de Marzo 2020
14. Publicación de los Contratos	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 de la **Superintendencia de Bancos de la Republica Dominicana** ubicada en la **Ave. México no. 52** en el horario de lunes a viernes en horario de **8:30 am a 4:30 pm**, en la fecha indicada en el Cronograma de la Licitación y en la página Web de la institución **www.sib.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.sib.gob.do**, o del portal administrado por el Órgano Rector, www.comprasdominicana.gov.do, deberá enviar un correo electrónico a **wsolis@sib.gob.do**, o en su defecto, notificar a la **División de**

Compras de la **Superintendencia de Bancos de la República Dominicana** 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

La entidad contratante deberá tener pendiente que, al momento de confeccionar el Pliego de Condiciones Específicas, deberá distribuirse la cantidad total de cada producto en diferentes renglones, en los casos en que una misma convocatoria abarque un número importante de unidades, con el objeto de estimular la participación de las micro, pequeñas y medianas empresas.

Item	Descripción	Cant.	Plazo	Presupuesto
1	MIGRACIÓN DE PLATAFORMA FIREWALLS	1	8 Semanas	16,000,000.00
2	IMPLEMENTACION DE UNA HERRAMIENTA PARA ESCANEO DE VULNERABILIDADES	1	2 Semanas	2,437,500.00
3	DESKTOP CENTRAL ENTEPRISE EDITION DE LA HERRAMIENTA MANAGEENGINE PARA LA ASISTENCIA REMOTA A USUARIOS FINALES	1	3 Semanas	2,431,560.00
4	ROBUSTECIMIENTO DE LA PLATAFORMA CITRIX NETSCALER	1	8 Semanas	11,100,600.00
5	DISPOSITIVOS PARA LA REDUNDANCIA DE LA CONECTIVIDAD DE LAS REDES DE DATOS ENTRE LOS DIFERENTES NIVELES	1	8 Semanas	800,000.00
6	RACK PDU MONITOREABLES	1	8 Semanas	317,160.00
7	RENOVACION CENTRAL TELEFONICA (CISCO CUCM)	1	4 Semanas	2,000,000.00
8	RENOVACION SOPORTE PLATAFORMA HPE	1	3 Semanas	3,809,224.00

1. MIGRACIÓN DE PLATAFORMA FIREWALLS

1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente la Superintendencia de Bancos (SIB) tiene implementado una plataforma de firewalls para la protección del perímetro de su red. Sin embargo, las amenazas persistentes y multivectoriales de hoy en día, los entornos de TI fluidos y también el aumento de la movilidad del usuario hacen que

la arquitectura actual de la plataforma del firewall no sea suficiente para mitigar los riesgos y las amenazas que puedan presentarse. Por esta razón, se hace necesario la implementación de una nueva plataforma de firewall de próxima generación, que proporcione una protección contra amenazas eficaz por niveles.

2. OBJETIVOS

2.1. Objetivo General

Migrar la plataforma de Firewalls existente en el perímetro de la red de la Superintendencia de Bancos (SIB).

2.2. Objetivos Específicos

- ✓ Inspeccionar el trafico entrante desde el perímetro
- ✓ Responder a ataques día cero.
- ✓ Responder a ataques de código malicioso.
- ✓ Proteger las aplicaciones de la SIB

3. FUNCIONALIDADES DE PLATAFORMA DE FIREWALLS

La solución debe consistir de appliances de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo;
Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7

- ✓ El hardware y software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser de tipo appliance.
- ✓ El software deberá ser ofrecido en su versión más estable y/o más avanzada
- ✓ La arquitectura de procesadores utilizado por la solución tiene que ser procesadores reprogramables, tipo FPGA, para garantizar que con futuras actualizaciones el equipo no quede obsoleto.

Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:

- ✓ Soporte de 4094 VLAN Tags 802.1q, tanto por dispositivo como en una sola interfaz
- ✓ Agregación de links 802.3ad
- ✓ Policy based routing o policy based forwarding;
- ✓ Ruteo multicast (PIM-SM)
- ✓ DHCP Relay
- ✓ DHCP Server
- ✓ Jumbo Frames
- ✓ La solución debe consistir de appliances de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo.

- ✓ Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3
- ✓ Soportar sub-interfaces ethernet lógicas.
- ✓ Debe soportar los siguientes tipos de NAT:
- ✓ Nat dinamico (Many-to-1)
- ✓ Nat dinámico (Many-to-Many)
- ✓ Nat estático (1-to-1)
- ✓ NAT estático (Many-to-Many)
- ✓ Nat estático bidireccional 1-to-1
- ✓ Traducción de porta (PAT)
- ✓ NAT de Origen
- ✓ NAT de Destino
- ✓ Soportar NAT de Origen y NAT de Destino simultáneamente
- ✓ Enviar log para sistemas de monitoreo externos, simultáneamente
- ✓ Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL;
- ✓ Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs;
- ✓ Seguridad contra anti-spoofing;
- ✓ Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);
- ✓ Debe soportar MP-BGP
- ✓ Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3);
- ✓ Soportar OSPF graceful restart;
- ✓ Debe ser capaz de balancear varios enlaces de internet sin el uso de políticas específicas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted...)
- ✓ Soportar BFD (bidirectional forward detection)
- ✓ Soportar LACP/LLDP Pre-negotiation
- ✓ Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Desencripción SSL y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.

- ✓ Debe contar con una herramienta para poder optimizar políticas de seguridad, detectar cuáles no se estén usando y por cuánto tiempo; poder aprender de las políticas aplicadas y sugerir que aplicaciones deberían aplicarse a las políticas en el NGFW. Dar estadísticas de uso, ancho de banda por aplicación, último hit de las aplicaciones, sobre cada política, con el objetivo de optimizar y mejorar la configuración del NGFW
- ✓ Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall,

sin necesidad de tener que hacer uso de contextos virtuales: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (L2), Capa 3 (L3) y modo Transparente

- ✓ Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red
- ✓ Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación
- ✓ Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas.
- ✓ Modo Transparente, para poder inspeccionar de datos en línea y tener visibilidad del control de tráfico en nivel de aplicación sobre 2 puertos en modo bridge/Transparente.
- ✓ Modo mixto de trabajo Sniffer, Transparente, L2 e L3 simultáneamente en diferentes interfaces físicas del mismo equipo.
- ✓ En el modo Transparente, debe poder soportar al menos 256 interfaces (fisicas y/o virtuales) sobre cada sistema virtual lógico (Contexto).
- ✓ Soporte a configuración de alta disponibilidad Activo/Pasivo e Activo/Activo:
- ✓ En modo transparente
- ✓ En layer 3
- ✓ La configuración en alta disponibilidad debe sincronizar
- ✓ Sesiones;
- ✓ Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QOS y objetos de red;
- ✓ Certificados de descripción
- ✓ Asociaciones de Seguridad de las VPNs
- ✓ Tablas FIB
- ✓ El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.
- ✓ Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.

- ✓ Debe poder inspeccionar protocolos como:
- ✓ GRE
- ✓ IPSEC no encriptado (NULL o AH)
- ✓ GPRS para GTP-U

El Next Generation Gateway debe ser capaz de soportar las siguientes aplicaciones de seguridad de próxima generación.

- ✓ Filtrado de URL
- ✓ IPS
- ✓ Sandboxing
- ✓ IPSec VPN

- ✓ Event Logs & Report
- ✓ QOS
- ✓ GEO Localización
- ✓ Identificación de Usuarios
- ✓ Control de aplicaciones

3.1. Capacidad (Throughput)

- ✓ Throughput de 18 Gbps medido con tráfico real (no es válido tomar mediciones ideales o de laboratorio) con la funcionalidad de Firewall habilitada.

- ✓ Throughput de 6Gbps medido con tráfico real (no es válido tomar mediciones ideales o de laboratorio) con las funcionalidades de Firewall, Control Aplicaciones e IPS habilitadas simultáneamente.

- ✓ Throughput de 6Gbps medido con tráfico real (no es válido tomar mediciones ideales o de laboratorio) con las funcionalidades de Firewall e IPS habilitadas simultáneamente.

- ✓ Throughput de 4 Gbps medido con tráfico real (no es válido tomar mediciones ideales o de laboratorio) con las funcionalidades de Firewall, Control de Aplicaciones, Filtrado URLs, IPS, Antivirus, Anti-Bot y Sandbox habilitadas simultáneamente.

3.2. Filtrado de URL

- ✓ El Security Gateway debe utilizar Stateful Inspection basado en el análisis granular de la comunicación y el estado de la aplicación para rastrear y controlar el flujo de red.
- ✓ El Security Gateway debe ser capaz de soportar los requerimientos de la Superintendencia de Bancos (SIB) de throughput, tasa de conexión, y conexiones concurrentes.
- ✓ Permite especificar la política por tempo, horario o determinado período (día, mes, año, día de la semana y hora)
- ✓ Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad
- ✓ Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y contra de quien está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local.
- ✓ Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio

- ✓ Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL
- ✓ Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función
- ✓ Debe soportar una cacheé local de URL en el appliance, evitando el delay de comunicación/validación de las URLs
- ✓ Debe poseer al menos 60 categorías de URL
- ✓ Debe soportar la creación de categorías URL custom
- ✓ Debe soportar la exclusión de URLs del bloqueo por categoría
- ✓ Debe permitir la customización de la página de bloqueo
- ✓ Debe permitir o bloquear y continuar (habilitando que el usuario acceso a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de "continuar" para permitirle seguir a ese site)
- ✓ Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios
- ✓ Debe evitar la fuga de credenciales desde o hacia sitios web, pudiendo tener granularidad en la configuración, es decir poder permitir o no el uso de credenciales de red internas en diferentes categorías de páginas web (estas categorías podrían ser: phising, redes sociales, foros, o categorías personalizadas por el cliente, etc), en incluso el uso indebido de los mismos dentro de la red del cliente. El objetivo de este requerimiento, es evitar que credenciales internas de la red sean publicadas en sitios de internet, inclusive sitios categorizados como desconocidos por el motor de categorización de filtros de URL.
- ✓ Debe poder actualizar de forma automática en 5 minutos o menos las categorías de malware y phising.
- ✓ La solución debe soportar control de acceso para al menos 150 servicios/protocolos predefinidos.
- ✓ Debe proporcionar estadísticas de recuento de reglas de seguridad a la aplicación de gestión.
- ✓ Debe permitir que las reglas de seguridad se apliquen en intervalos de tiempo para ser configurados con una fecha / hora de caducidad.
- ✓ La comunicación entre los Management Servers y los Security Gateway debe ser cifrada y autenticada con certificados PKI.
- ✓ El firewall debe soportar métodos de autenticación de usuario, cliente y sesión.
- ✓ Los siguientes esquemas de autenticación de usuario deben ser soportados por el security Gateway y el módulo de VPN: tokens (ie – Secure ID), TACACS, RADIUS, and digital certificates.
- ✓ La solución debe incluir un usuario local de base de datos para permitir autenticación y autorización del usuario sin necesidad de un dispositivo externo.
- ✓ La solución debe soportar DHCP, servidor y relay.
- ✓ La solución debe proporcionar proxy HTTP & proxy HTTPS.

- ✓ La solución debe incluir la opción de trabajar en modo Transparente/Bridge.
- ✓ La solución debe proporcionar Alta disponibilidad de los Gateways y reparto de cargas con sincronización de estado.

3.3. Sandboxing

- ✓ Poseer la capacidad de análisis de amenazas no conocidas
- ✓ Debido a los Malware hoy en día se debe ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada deber poseer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta
- ✓ El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado;
- ✓ Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis
- ✓ Soportar el análisis de por lo menos 60 (sesenta) tipos de comportamientos maliciosos para el análisis de la amenaza no conocida
- ✓ Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7
- ✓ Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB
- ✓ El sistema de análisis “In Cloud” o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red)
- ✓ El sistema automático de análisis "In Cloud" o local debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware
- ✓ Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración;
- ✓ Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración
- ✓ Debe permitir visualizar los resultados de los análisis de malware de día Zero en los diferentes sistemas operacionales soportados
- ✓ Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración

- ✓ Soportar el análisis de archivos ejecutables, DLLs, ZIP y encriptados en SSL en el ambiente controlado
- ✓ Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado
- ✓ La solución debe poder emular archivos ejecutables, archivos, documentos, JAVA y flash, incluidos los siguientes:
- ✓ 7z, Cab, Csv, Doc, Docm, Docx, Dot, Dotm, Dotx, Exe, Jar, Pdf, Potx, Pps, Ppsm, Ppsx, Ppt, Pptm, Pptx, Rar, Rtf, Scr, Swf, Tar, Tgz, Xla, Xls, Xlsb, Xlsm, Xlsx, Xlt, Xltm, Xltx, Xlw,
- ✓ El NGFW debe enviarle archivos previamente desconocidos a un sandbox en la nube para la prevención de amenazas desconocidas.
- ✓ sandbox debe tener los siguientes tipos de análisis: Machine Learning, Análisis Estático, Análisis Dinámico y Bare Metal.
- ✓ sandbox debe generar el veredicto y la protección necesaria en 5 minutos o menos.
- ✓ Como parte de la protección el sandbox debe generar las siguientes protecciones: Firmas de antivirus, Firmas de DNS y Firmas de URL Filter, el NGFW debe poder buscar actualizaciones de nuevas protecciones del sandbox cada minuto.
- ✓ Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.
- ✓ Debe poder dar veredictos distintos, como mínimo:
- ✓ Malicioso
- ✓ Grayware
- ✓ Benigno
- ✓ Phising
- ✓ En caso de detectar una forma de evasión de máquina virtual, debe poder enviar de forma automática a revisión en modo Bare Metal (maquinas físicas)

3.3 Threat Prevention

- ✓ Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware).
- ✓ Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
- ✓ Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo.
- ✓ Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente.

- ✓ Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo.
- ✓ Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma por firma.
- ✓ Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.
- ✓ Debe permitir el bloqueo de vulnerabilidades.
- ✓ Debe permitir el bloqueo de exploits conocidos.
- ✓ Debe incluir seguridad contra ataques de negación de servicios.
- ✓ Deberá poseer los siguientes mecanismos de inspección de IPS:
- ✓ Análisis de parones de estado de conexiones;
- ✓ Análisis de decodificación de protocolo;
- ✓ Análisis para detección de anomalías de protocolo;
- ✓ Análisis heurístico
- ✓ IP Defragmentation
- ✓ Re ensamblado de paquetes de TCP;
- ✓ Bloqueo de paquetes malformados.
- ✓ Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc
- ✓ Detectar y bloquear el origen de portscans
- ✓ Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones;
- ✓ Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re ensamblado de paquetes de TCP y bloqueo de paquetes malformados
- ✓ Posea firmas específicas para la mitigación de ataques DoS
- ✓ Posea firmas para bloqueo de ataques de buffer overflow
- ✓ Posea firmas de C2 (Comando y control) generadas de forma automática.
- ✓ Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- ✓ Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3
- ✓ Soportar bloqueo de archivos por tipo
- ✓ Identificar y bloquear comunicaciones como botnets
- ✓ Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos)
- ✓ Debe soportar referencia cruzada como CVE
- ✓ Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas:
- ✓ Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antispyware

- ✓ Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes
- ✓ Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos.
- ✓ Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- ✓ Los eventos deben identificar el país de donde partió la amenaza;
- ✓ Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
- ✓ Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables. maliciosos.
- ✓ Rastreo de virus en pdf.
- ✓ Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.)
- ✓ Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad, etc, o sea, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por Usuarios, Grupos de usuario, origen, destino, zonas de seguridad.

3.4 Anti-Bot, Anti-Virus

- ✓ El suplidor debe tener una aplicación Anti-Bot y Anti-Virus en el Firewall de Nueva Generación.
- ✓ La aplicación Anti-Bot debe ser capaz de detectar y parar un comportamiento de red anormal o sospechoso.
- ✓ La aplicación Anti-Bot debe utilizar un motor de detección de múltiples niveles, el cual incluye reputación de IPs, URLs y direcciones DNS y detectar patrones de comunicaciones bot.
- ✓ La solución debe soportar detección y prevención de virus tipo Cryptors & ransomware y sus variantes (Cryptolocker, CryptoWall…) a través del uso de análisis dinámico y/o estático.
- ✓ La solución debe tener mecanismos para proteger contra ataque spear phishing.
- ✓ La solución debe tener mecanismos para proteger contra ataques Water Holings.

La solución debe tener capacidades de detección y prevención para escondites Command & Control (C&C) DNS:

- ✓ Buscar patrones de tráfico C&C, no sólo en su destino DNS.
- ✓ Realizar Reverse Engineering al malware para descubrir su Generación de Nombre de Dominio (DGA).
- ✓ Funcionalidad de trampa de DNS como parte de la prevención de amenazas, asistiendo en el descubrimiento de hosts infectados generando comunicación C&C.

- ✓ La solución debe tener capacidades de detección y prevención de ataques de DNS tunneling.
- ✓ La solución debe permitir administrar la política de Anti-Bot y Anti-Virus desde una consola centralizada.
- ✓ La aplicación de Anti-Bot y Anti-Virus deben tener un mecanismo de correlación de evento y reportes centralizado.
- ✓ La aplicación Anti-Virus debe ser capaz de prevenir el acceso a websites maliciosos.
- ✓ La aplicación Anti-Virus debe ser capaz de inspeccionar tráfico cifrado SSL.
- ✓ El Anti-Bot y Anti-Virus deben tener actualizaciones en tiempo real desde un servicio basado en la nube.
- ✓ El Anti-Virus debe ser capaz de detener archivos maliciosos entrantes.
- ✓ El Anti-Virus debe ser capaz de escanear archivos comprimidos.
- ✓ Las políticas de Anti-Virus y Anti-Bot deben ser gestionadas centralmente con aplicación y configuración granular de políticas.
- ✓ El Anti-Virus debe soportar más de 50 motores de AV basados en la nube.
- ✓ El Anti-Virus debe soportar el escaneo de enlaces dentro de los correos electrónicos.
- ✓ El Anti-Virus debe escanear archivos que están pasando sobre protocolo CIFS.

3.5 Inspección SSL (Inbound/Outbound)

- ✓ La solución ofrece soporte para el Descifrado/Inspección SSL con alto rendimiento a través de todas las tecnologías de mitigación de amenazas.
- ✓ La solución debe soportar Perfect Forward Secrecy (PFS, suites de cifrado ECDHE)
- ✓ La solución debe soportar AES-NI, AES-GCM para rendimiento mejorado.
- ✓ La solución debe aprovechar la base de datos del filtro de URL para permitir al administrador crear políticas granulares de inspección https.
- ✓ La solución puede inspeccionar el filtro URL sobre HTTPS sin requerir el descifrado de SSL.
- ✓ Deberá soportar controles por zona de seguridad
- ✓ Controles de políticas por puerto y protocolo.
- ✓ Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
- ✓ Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.
- ✓ Control de políticas por código de País (Por ejemplo: AR, BR, USA, UK, RUS).
- ✓ Control, inspección y desencripción de SSL por política para tráfico y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras)
- ✓ Se permite la entrada (Inbound) y Salida (Outbound).
- ✓ Debe soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound)

- ✓ Debe desencriptar tráfico Inbound y Outbound en conexiones negociadas con TLS 1.2
- ✓ Debe desencriptar tráfico que use certificados ECC (como ECDSA)
- ✓ Control de inspección y desencripción de SSH por política;
- ✓ La plataforma de seguridad debe implementar copia del tráfico desencriptado (SSL uso de appliance externo, específico para la desencripción de (SSL y TLS), con copia del tráfico desencriptado tanto para el firewall, como para otras soluciones de análisis externas.
- ✓ Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, y reg
- ✓ Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo)
- ✓ QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
- ✓ Soporte a objetos y Reglas IPV6.
- ✓ Soporte a objetos y Reglas multicast.
- ✓ Soporte SD-WAN
- ✓ Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente

3.6 IPSec VPN

- ✓ Autoridades de Certificación Internas y Externas deben ser soportadas.
- ✓ La solución debe soportar criptografía 3DES y AES-256 para la Fase 1 y II IKEv2 más “Suite-B-GCM-128” y “Suite-B-GCM-256” para Fase II
- ✓ La solución debe soportar al menos los siguientes Grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit), Grupo 19 y Grupo 20.
- ✓ Soportar VPN Site-to-Site y Cliente-To-Site;
- ✓ Soportar IPSec VPN;
- ✓ Soportar SSL VPN;
- ✓ La VPN IPSEc debe soportar:
- ✓ DES y 3DES;
- ✓ Autenticación MD5 e SHA-1;
- ✓ Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
- ✓ Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- ✓ AES 128, 192 e 256 (Advanced Encryption Standard)
- ✓ Debe permitir SSO via Kerberos
- ✓ Autenticación vía certificado IKE PKI.
- ✓ Debe ser compatible con la Suite B de protocolos de NSA
- ✓ Debe poseer interoperabilidad como los siguientes fabricantes:
- ✓ Cisco
- ✓ Checkpoint;
- ✓ Juniper;
- ✓ Palo Alto Networks;

- ✓ Fortinet;
- ✓ Sonic Wall

Las VPN SSL deben soportar:

- ✓ Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB
- ✓ Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente
- ✓ La asignación de dirección IP en los clientes remotos de VPN
- ✓ La asignación de DNS en los clientes remotos de VPN
- ✓ Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario
- ✓ Deber permitir criar políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL
- ✓ Las VPN SSL deben soportar proxy arp y el uso de interfaces PPPOE;
- ✓ Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local
- ✓ Permite establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon
- ✓ Soporte de lectura y verificación de CRL (certificate revocation list);
- ✓ Permite la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles SSL
- ✓ El agente de VPN a ser instalado en los equipamientos desktop y laptops, debe ser capaz de ser distribuido de manera automática vía Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN
- ✓ El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario
- ✓ Debe permitir que las conexiones como VPN SSL sean establecidas de las siguientes formas
- ✓ Antes del usuario autenticarse en la estación
- ✓ Después de la autenticación del usuario en la estación
- ✓ Bajo demanda del usuario
- ✓ Deberá mantener una conexión segura con el portal durante la sesión

El agente de VPN SSL client-to-site debe ser compatible al menos con:
Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X; Apple iOS, Android, Linux, Windows 10 UWP y Google Chrome OS 45 superior

- ✓ El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente
- ✓ Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.

- ✓ Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa
- ✓ Debe soportar VPN SSL sin el uso de cliente
- ✓ Esta función no debe estar basada en Java
- ✓ Debe poder integrarse con soluciones MDM de terceros (por ejemplo, AirWatch)
- ✓ La administración de la solución debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta
- ✓ En el caso de que sea necesaria la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operacionales Windows y Linux
- ✓ La administración debe permitir/hacer
- ✓ Creación y administración de políticas de firewall y control de aplicaciones
- ✓ Creación y administración de políticas de IPS y Anti-Spyware;
- ✓ Creación y administración de políticas de filtro de URL
- ✓ Monitoreo de logs
- ✓ Herramientas de investigación de logs;
- ✓ Debugging
- ✓ Captura de paquetes.
- ✓ Debe permitir el acceso concurrente de administradores;
- ✓ Debe tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos;
- ✓ Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificación de Reglas
- ✓ Debe permitir monitorear vía SNMP fallas en el hardware, inserción o remoción de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de túneles establecidos de VPN cliente-to-site, porcentaje de utilización en referencia al número total soportado/licenciado y número de sesiones establecidas
- ✓ Debe permitir el bloqueo de alteraciones, en el caso de acceso simultáneo de dos o más administradores
- ✓ Debe permitir la definición de perfiles de acceso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creación de usuarios, alteración de configuraciones
- ✓ Debe permitir la autenticación integrada con Microsoft Active Directory y servidor Radius
- ✓ Debe permitir la localización de donde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos
- ✓ Debe poder atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS
- ✓ Debe permitir la creación de Reglas que estén activas en un horario definido
- ✓ Debe permitir la creación de Reglas con fecha de expiración;
- ✓ Debe poder realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada
- ✓ Debe soportar el Rollback de Sistema operativo para la última versión local

- ✓ Debe poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración
- ✓ Debe poder validar las Reglas antes de las aplicaciones;
- ✓ Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing)
- ✓ Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.
- ✓ Debe posibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)
- ✓ Debe permitirá la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo y el horario de la alteración
- ✓ Deberá tener la capacidad de generar un gráfico que permita visualizar los cambios en la utilización de aplicaciones en la red en lo que se refiere a un período de tiempo anterior, para permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con relación al pasado
- ✓ Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución
- ✓ Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes

3.7 GEO Localización

- ✓ Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
- ✓ Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
- ✓ Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.

3.8 QOS

Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la solución, a la vez de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.

- ✓ Soportar la creación de políticas de QoS por:
- ✓ Dirección de origen
- ✓ Dirección de destino
- ✓ Por usuario y grupo de LDAP/AD.
- ✓ Por aplicaciones, incluyendo, más no limitando a Skype, Bittorrent, YouTube y Azureus;
- ✓ Por puerto;
- ✓ El QoS debe permitir la definición de clases por:
- ✓ Ancho de Banda garantizado

- ✓ Ancho de Banda Máximo
- ✓ Cola de prioridad.
- ✓ Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- ✓ Soportar marcación de paquetes Diffserv, inclusive por aplicaciones;
- ✓ Disponer de estadísticas Real Time para clases de QoS.
- ✓ Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.

3.9 Identificación de Usuarios

- ✓ Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local.
- ✓ Debe poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- ✓ Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
- ✓ Debe poseer integración con TACACS+
- ✓ Debe posea integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.
- ✓ Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC vía syslog, para la identificación de direcciones IP y usuarios
- ✓ Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal)
- ✓ Soporte a autenticación Kerberos.
- ✓ Soporte SAML 2.0
- ✓ La solucion ofrecida debe soportar e incluir múltiples factores de autenticación (como por ejemplo usuario y password + 2FA hard token + 2FA soft token + portal cautivo) para poder utlizarlo tanto en aplicación web como en aplicaciones cliente servidor.
- ✓ Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios
- ✓ Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.

3.10 Control de aplicaciones

- ✓ Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo, con las siguientes funcionalidades
- ✓ Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
- ✓ Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail
- ✓ Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc
- ✓ Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, más no limitando a RDP en el puerto 80 en vez del 389
- ✓ Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan cifrado propietario
- ✓ Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones cifradas, tales como Skype y ataques mediante el puerto 443.
- ✓ Para tráfico Cifrado (SSL y SSH), debe permitir la desencripción de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante
- ✓ Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, más no limitado a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, más no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas
- ✓ Debe Identificar el uso de tácticas evasivas vía comunicaciones cifradas
- ✓ Debe Actualizar la base de firmas de aplicaciones automáticamente;
- ✓ Debe Reconocer aplicaciones en IPv6;
- ✓ Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD

- ✓ Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios
- ✓ Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas
- ✓ Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico
- ✓ Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas
- ✓ Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la empresa
- ✓ La creación de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos:
  HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body.
- ✓ El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones;
- ✓ Debe alertar al usuario cuando una aplicación fuera bloqueada
- ✓ Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones
- ✓ Debe posibilitar la diferenciación de tráficos Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/políticas para los mismos
- ✓ Debe posibilitar la diferenciación de tráficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos
- ✓ Debe posibilitar la diferenciación y control de partes de las aplicaciones como por ejemplo permitir Gtalk chat y bloquear la transferencia de IM (mensajería instantánea)
- ✓ Debe posibilitar a diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/políticas para los mismos
- ✓ Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
- ✓ Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- ✓ Nivel de riesgo de las aplicaciones.
- ✓ Categoría y sub-categoría de aplicaciones.
- ✓ Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
- ✓ Debe poder monitorear aplicaciones SaaS (Software as a service) tanto via GUI como en reporte predefinido

3.11 Gestión de Seguridad

- ✓ La aplicación de gestión de seguridad debe ser capaz de co-existir en el security Gateway como una opción
- ✓ La aplicación de gestión de seguridad debe soportar cuentas de administrador basadas en roles
- ✓ La solución debe incluir un canal de comunicaciones seguro cifrado basado en Certificados entre todos los componentes distribuidos pertenecientes a un dominio de gestión
- ✓ La solución debe incluir una Autoridad Certificadora x.509 interna que pueda generar certificados a los gateways y usuarios para permitir la autenticación en las VPNs
- ✓ La solución debe incluir la capacidad de utilizar Autoridades Certificadoras externas, que soporte los estándares PKCS#12, CAPI o Entrust
- ✓ Todas las aplicaciones de seguridad deben ser gestionadas desde una consola central
- ✓ La gestión debe proveer un contador de reglas de seguridad tocadas en la política de seguridad
- ✓ La solución debe incluir una opción de búsqueda capaz de buscar qué objeto de red contiene una IP específica o parte de ella
- ✓ La solución debe incluir la opción de separar las reglas utilizando etiquetas o títulos de sección para organizar mejor la política
- ✓ La solución debe tener un mecanismo de verificación de política de seguridad antes de la instalación de la política.
- ✓ La solución debe tener un mecanismo de control de revisión de política
- ✓ La solución debe proporcionar la opción de añadir Alta Disponibilidad de la Gestión, utilizando un servidor de gestión standby que es sincronizado automáticamente con el activo, sin la necesidad de un dispositivo de almacenamiento externo
- ✓ La solución debe incluir un mapa comprensivo con todos los objetos de red y sus conexiones que pueda ser exportado a Microsoft Visio o un archivo de imagen
- ✓ La solución debe incluir la capacidad de distribuir centralmente y aplicar nuevas versiones de software del Gateway.
- ✓ La solución debe incluir una herramienta que administre centralmente las licencias de todos los gateways controlados por la estación de gestión
- ✓ El GUI de gestión debe tener la habilidad de excluir fácilmente una dirección IP desde la definición de firmas de IPS
- ✓ El Visor de Logs debe tener la capacidad de excluir fácilmente una dirección IP desde los logs de IPS cuando es detectado como un falso positivo
- ✓ El GUI de gestión debe tener la capacidad de llegar fácilmente a la definición de firmas de IPS desde los logs de IPS
- ✓ El Visor de Logs debe tener la capacidad de ver todos los logs de seguridad (FW, IPS, URLF..) en un panel de vistas
- ✓ El Visor de Logs debe tener la capacidad en el visor de log de crear filtros utilizando los objetos predefinidos (hosts, red, grupos, usuarios, etc.)

- ✓ El Visor de Logs debe tener la capacidad de crear y salvar filtros personalizados para usar en un momento posterior.

3.12 Actualizaciones de Prevención de Amenazas

- ✓ El suplidor debe proporcionar los detalles de su mecanismo de actualización de prevención de amenazas y su capacidad de manejar ataques día cero a través de todas las aplicaciones de prevención de amenazas (IPS, Application Control, URL Filtering, Anti-Bot y Anti-Virus).

- ✓ El suplidor debe proporcionar detalles en la re-categorización de URL, bajo las circunstancias de que un website haya sido comprometido y posiblemente distribuido malware.

- ✓ El suplidor debe tener la capacidad de proporcionar manejo de incidentes.

3.13 Monitoreo & Logging

- ✓ El logging central debe ser parte del sistema de gestión. Alternativamente los administradores pueden instalar Servidores de Logs dedicados.
- ✓ La solución debe proporcionar la opción de correr en el servidor de gestión o en un servidor dedicado.
- ✓ La solución debe ser capaz de correr sobre Open Servers X86 listados en una lista de compatibilidad de hardware.
- ✓ La solución debe tener la capacidad de registrar los logs de todas las reglas.
- ✓ El visor de logs debe tener capacidad de búsqueda indexada.
- ✓ La solución debe tener la capacidad de registrar los logs de todas las aplicaciones de seguridad integradas en el Gateway, incluyendo IPS, Control de Aplicaciones, Filtro de URL, Anti-Virus, Anti-Bot, Anti-Spam, Identidad de Usuario.
- ✓ La solución debe incluir un mecanismo automático de captura de paquete para eventos IPS para proporcionar mejor análisis forense.
- ✓ La solución debe proporcionar logs diferentes para las actividades regulares de usuarios y para actividades de gestión.
- ✓ La solución debe ser capaz de moverse desde el registro de log de seguridad a la regla de la política en un solo click.
- ✓ Para cada regla evaluada o tipo de evento la solución debe proporcionar al menos las siguientes opciones de eventos: Log, alert, SNMP trap, email y ejecutar un script definido por el usuario.
- ✓ Los logs deben tener un canal seguro para transferir el logging para evitar eavesdropping, la solución debe ser autenticada y cifrada.
- ✓ Los logs deben ser transferidos de manera segura entre el Gateway y el servidor de gestión o dedicado a logs y la consola de visor de logs en la PC del administrador.
- ✓ La solución debe incluir la opción para bloquear dinámicamente una conexión activa desde la interfaz gráfica de logs sin tener que modificar la base de reglas.
- ✓ La solución debe soportar la exportación de logs en formato de base de datos.

- ✓ La solución debe soportar el cambio automático del archivo de log, basado en un tiempo definido o tamaño del archivo.
- ✓ La solución debe soportar añadir excepciones a la aplicación de IPS desde el registro de log.
- ✓ La solución debe ser capaz de asociar un usuario y nombre de la máquina a cada registro de log.
- ✓ La solución debe incluir una interfaz gráfica de monitoreo que permita monitorear fácilmente los status de los gateways.
- ✓ La solución debe proporcionar la siguiente información de sistema para cada Gateway: OS, uso de CPU, uso de memoria, particiones de disco y porcentaje de espacio de disco duro libre.
- ✓ La solución debe proporcionar el status de cada componente.
- ✓ La solución debe incluir el status de todos los túneles VPN, site-to-site y client-to-site.
- ✓ La solución debe incluir ajustes de límites personalizables para tomar acciones cuando cierto límite es alcanzado en un Gateway. Las acciones deben incluir: Log, alert, enviar un SNMP trap, enviar un email y ejecutar una alerta definida por el usuario.
- ✓ La solución debe incluir gráficas preconfiguradas para monitorear la evolución en el tiempo del tráfico y contadores de sistemas: reglas de seguridad top, usuarios P2P top, túneles VPN, tráfico de red y otras informaciones. La solución debe proporcionar la opción de generar nuevos gráficos personalizables con diferentes tipos de charts.
- ✓ La solución debe incluir la opción de registrar tráfico y vistas de sistema a un archivo para ser visto luego en cualquier momento.
- ✓ La solución debe ser capaz de reconocer problemas de conectividad y malfuncionamiento, entre dos puntos conectados a través de una VPN, y registrar y alertar cuando un túnel VPN esté abajo.

3.14 Gestión y Reportes

- ✓ La solución debe proporcionar la capacidad de ser administrada centralmente.
- ✓ Tras la detección de archivos maliciosos, se debe generar un informe detallado para cada uno de los archivos maliciosos.

El informe detallado debe incluir:

- ✓ Capturas de pantalla
- ✓ Líneas de tiempo
- ✓ Creación / modificación de claves de registro
- ✓ Creación de archivos y procesos.
- ✓ Actividad de red detectada

3.15 Correlación de Eventos & Reportes

- ✓ La solución debe estar totalmente integrada a la aplicación de gestión.
- ✓ La solución debe incluir una herramienta para correlacionar eventos de todas las características del Gateway y dispositivos de terceros.

- ✓ La solución debe permitir la creación de filtros basados sobre cualquier característica del evento como seguridad de aplicación, IP fuente y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, país de origen y destino, etc.
- ✓ La aplicación debe tener un mecanismo para asignar estos filtros a diferentes líneas gráficas que son actualizadas en intervalos regulares mostrando todos los eventos que coincidan con el filtro.
- ✓ La aplicación de correlación de eventos debe suplir una vista gráfica de eventos basados en el tiempo.
- ✓ La solución debe mostrar la distribución de eventos por país sobre un mapa.
- ✓ La solución debe permitir al administrador agrupar eventos basados en cualquiera de sus características, incluyendo niveles de anidación y exportar a PDF.
- ✓ La solución debe incluir la opción de buscar dentro de la lista de eventos, hacer drill down a los detalles para investigación y forense.
- ✓ La solución debe incluir la opción de generar automáticamente gráficos o tablas con la distribución del evento, fuente y destino.
- ✓ La solución debe detectar ataques de Denegación de Servicio correlacionando eventos de todas las fuentes.
- ✓ La solución debe detectar el login de un administrador a horas irregulares.
- ✓ La solución debe detectar ataques de obtención de credenciales.
- ✓ La solución debe reportar sobre todas las instalaciones de políticas de seguridad.
- ✓ La solución debe incluir reportes predefinidos por hora, diario, semanal y mensual. Incluir los eventos principales, fuentes principales, destinos principales, servicios principales, fuentes principales y sus eventos principales, destinos principales y sus eventos principales, y servicios principales y sus eventos principales.
- ✓ La herramienta de reporte debe soportar al menos 25 filtros que permitan personalizar un reporte predefinido a las necesidades del administrador.
- ✓ La solución debe soportar la programación de reportes automáticos para información que necesite ser extraída regularmente (diario, semanal, mensual). La solución debe permitir al administrador definir la fecha y tiempo en que el sistema de reportes comienza a generar el reporte programado.
- ✓ La solución debe soportar los siguientes formatos de reporte: HTML, CSV y MHT.
- ✓ La solución debe soportar la distribución automática de reporte por email, subir a un servidor FTP/Web y un script externo personalizado de distribución de reportes.
  El sistema de reportes debe proporcionar información consolidada acerca
- ✓ El volumen de conexiones que son bloqueadas por reglas de seguridad
- ✓ Fuentes principales de conexiones bloqueadas, sus destinos y servicios
- ✓ Reglas principales utilizadas por la política de seguridad.
- ✓ Ataques de seguridad principales detectados por el punto de aplicación (perímetro) determinando las fuentes y destinos principales.
- ✓ Número de políticas instaladas y desinstaladas en el punto de aplicación.
- ✓ Servicios de red principales

- ✓ Actividad web por usuario detallando los sitios principales visitados y los usuarios web principales.
- ✓ Servicios principales que crearon mayor carga para el tráfico cifrado.
- ✓ Usuarios principales de VPN que realizan las conexiones de más larga duración

3.16 Portal de Administración

- ✓ La solución debe incluir un acceso a través de browser para observar en modo sólo lectura las políticas de seguridad, gestionar los logs de firewall y los usuarios para proporcionar acceso a ejecutivos y auditores sin la necesidad de utilizar la aplicación de administración.
- ✓ La solución debe incluir soporte SSL y puerto configurable.

4. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- ✓ Estas aplicaciones deben ser suplidas y manejadas exclusivamente por el proveedor.
- ✓ El proveedor debe suplir las certificaciones de la industria de la solución.
- ✓ El proveedor debe diseñar y presentar para su aprobación un plan de trabajo, detalle de la metodología a utilizar y cronograma.
- ✓ El proveedor debe migrar e implementar la plataforma de Firewall de la institución una vez sea revisado y aprobado por el personal de la SIB
- ✓ La solución debe de estar en el cuadrante líder del cuadrante mágico de Gartner para Enterprise Network Firewalls.
- ✓ El proveedor debe ofrecer 40 horas de entrenamiento de curso oficial aprobado por el fabricante del producto, para al menos 3 personas.

5. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- ✓ Propuesta de plataforma de Next Generation Firewall
- ✓ Plan de trabajo de migración de plataforma de Firewalls
- ✓ Plataforma de Firewall de la Superintendencia de Bancos en funcionamiento
- ✓ Documento de cierre de proyecto que contenga las configuraciones y pasos realizados durante la implementación de la plataforma de Firewalls.

6. PERFIL PROFESIONAL:

- ✓ El proveedor del software del Gateway debe tener al menos 10 años de experiencia en el mercado de seguridad y proporcionar referencias sobre proyectos exitosos en clientes.
- ✓ El proveedor debe proporcionar evidencia de liderazgo año tras año en firewalls para empresa, firewalls basada en datos independientes de la seguridad de la industria.

2. IMPLEMENTACION DE UNA HERRAMIENTA PARA ESCANEO DE VULNERABILIDADES

1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente la SIB necesita una herramienta que permita la evaluación de vulnerabilidades de los activos críticos de la institución con el fin de identificar con un reporte sistemático con las vulnerabilidades en cuestión de seguridad que se tienen en una infraestructura. La intención es proteger en el mejor porcentaje posible la seguridad de la información ante el ataque de un ente externo. En tal sentido se necesita una herramienta para evaluar los equipos críticos informáticos existentes y así lograr identificar y reparar cualquier imprevisto con rapidez y facilidad, incluso hasta fallas de software, parches faltantes, malware y configuraciones erróneas.

2. OBJETIVOS

a. Objetivo General

Implementar una herramienta para el escaneo de vulnerabilidades en la Superintendencia de Bancos.

b. Objetivos Específicos

Identificar riesgos, vulnerabilidades o fallas de seguridad sobre los sistemas operativos de la organización.

Reparar cualquier vulnerabilidad con rapidez, antes de que esta sea explotada.

3. FUNCIONALIDADES DE PLATAFORMA DE ESCANEO DE VULNERABILIDADES

- El producto debe integrar plenamente la exploración y el cumplimiento de licencias para incluir combinado y consolidación de datos, análisis y consultas.
- El producto debe incluir una capacidad integrada modo activo / pasivo de descubrimiento para lograr plena visibilidad de la vulnerabilidad y el cumplimiento.
- El producto debe proporcionar la exploración basado tanto en sin agentes y mediante agente.
- El producto debe proporcionar normalización de registros (logs) integrado y en tiempo real y recopilación de estos eventos para reporte y análisis forense.

ARQUITECTURA

- El producto debe proporcionar un servidor centralizado para la recogida y gestión de la información de seguridad que reside localmente o dentro de la red de la organización.
- El producto debe proporcionar la capacidad para desplegar una arquitectura por niveles de varias consolas de ser necesario.
- El producto debe centralizar y automatizar la actualización de vulnerabilidad y amenaza en sus sensores, y la inteligencia se debe actualizar desde el proveedor en un modo diario.
- El producto debe proporcionar un proceso de actualización en línea (Offline) para actualizar el sensor dentro de redes aisladas o “airgap”.
- El producto debe proporcionar un modelo de almacenamiento integrado que no se base o requiera licenciamiento de base de datos de un tercero.
- El producto debe ser configurable para retener resultados por un período de tiempo después de lo cual los resultados se expiren y sean purgados de la base de datos automáticamente según definido y configurable.
- El servidor debe proporcionar una completa API para scripting automatizado de digitalización y la exportación de los datos de seguridad.
- El licenciamiento del producto debe permitir un servidor de reserva para ser sincronizado con el servidor principal de computación por desastres. “Active / Standby”
- La solución debe permitir analizar pasivamente el tráfico de red para el descubrimiento de activos y la identificación de vulnerabilidades en infraestructura crítica y sistemas integrados, que requieren un enfoque no intrusivo para la gestión de vulnerabilidades.
- La solución debe proporcionar una visibilidad continua de los sistemas que se ejecutan en su entorno, incluidos los dispositivos IoT (Internet of Things), permitiendo a los usuarios evaluar rápidamente los activos y los riesgos que representan para su entorno mediante dashboards en informes de IoT preconstruidos.
- La solución debe proporcionar actualizaciones frecuentes de inteligencia de vulnerabilidad y amenaza, análisis avanzado, políticas de seguridad / cumplimiento, en forma de paneles de control fáciles de interpretar, informes y tarjetas de informe de aseguramiento.
- La solución debe proporcionar monitoreo en tiempo real de la red y la actividad del host, lo que permite un análisis avanzado de la vulnerabilidad, la amenaza, la actividad de la red y la información de eventos para brindar una visión continua de la exposición a la seguridad dentro de un entorno.

- La solución debe permitir identificar rápida y fácilmente los sistemas de mayor riesgo en su red a través de paneles de priorización personalizables. Los activos identificados como los más vulnerables, los más infectados con malware, con mayores infracciones de políticas, en estatus de incumplimiento, etc. pueden identificarse rápidamente para ayudar a los administradores a tomar las decisiones más prioritarias sobre los esfuerzos de administración y mitigación.

- La solución debe ofrecer una amplia gama de integraciones preconstruidas. De igual manera, debe ofrecer una interfaz de programación de aplicaciones (API) y un kit de desarrollo de software (SDK) completamente documentados y fáciles de usar para ayudar a la exportación e importación de datos de vulnerabilidad, activos, amenazas y otros.

- La solución debe permitir el descubrimiento en vivo de todos los activos, la visibilidad continua de la seguridad y la exposición de esos activos, el contexto de cualquier exposición para priorizar la remediación y la visión estratégica para crear un programa basado en métricas que cuantifique y mida la exposición de estos.

- La solución debe permitir la administración de sensores activos y pasivos, el escaneo de aplicaciones web.

- La solución debe automatizar la evaluación de los controles técnicos de ISO / IEC 27001/27002, NIST Cybersecurity Framework, NIST SP 800-171 y CIS Critical Security Controls. Debe contener paneles e informes totalmente personalizables permiten al usuario medir, visualizar y comunicar de manera efectiva el cumplimiento de estos controles de seguridad.

- La solución debe proporcionar numerosos paneles de control ejecutivos, informes y tarjetas de informe de aseguramiento que permiten a la gerencia evaluar rápidamente el riesgo para su entorno. Los informes ejecutivos deben incluir información de vulnerabilidad resumida por tipo, gravedad, activo, explotabilidad y recientemente corregida para brindar a la administración una visión general integral del riesgo.

CONTROL DE ACCESO

- El producto debe proporcionar control de acceso basado en roles y perfiles con suficiente granularidad para controlar a los usuarios el acceso a determinados conjuntos de datos y la funcionalidad que está disponible para los usuarios.

- El producto debe permitir a los administradores definir nuevos roles basados en funciones de trabajo y los niveles adecuados de acceso a la funcionalidad. Adicional a los sugeridos por el fabricante.

- El producto debe integrarse con LDAP para la autenticación de usuarios.

- El producto debe integrarse con LDAP para la hacer consultas que faciliten creación de listas de activos.
- El producto debe ser compatible con auditoria detallada de la actividad del usuario.
- El producto debe permitir a los administradores limitar el acceso en función de cada usuario a listas específicas de activos, políticas de análisis, y repositorios con los datos de vulnerabilidad.
- El producto debe permitir a los administradores asignar los recursos en función de cada usuario, tales como políticas de análisis, las listas de activos, consultas y credenciales pre-definidas y compartidas.
- El producto debe permitir a los administradores limitar los permisos de exploración para la exploración completa, escanear mediante políticas específicas, o denegar la exploración.
- El producto debe incluir la posibilidad de programar ventanas de mantenimiento de escaneo en forma de evitar el análisis durante las horas restringidas. (Blackout Windows)
- producto debe ser compatible con definición de organizaciones lógicas con plena separación de datos entre los diferentes clientes de la organización. (Multi-Tenancy).
- El producto debe proporcionar la capacidad para definir rangos restringidos de direcciones IP para cada organización.
- El producto debe proporcionar la capacidad de restringir los permisos de flujo de trabajo para incluir aceptar y redefinir (recast), riesgo de vulnerabilidades en la organización.

ESCANEADO DISTRIBUIDO

- El producto debe ser compatible con una variedad de plataformas para el motor de exploración a incluir Windows, Linux, Mac OS, así como dispositivos virtuales o basadas en hardware.
- La solución deberá poder ejecutar una exploración pasiva mediante el análisis de red a través de un puerto espejo para el descubrimiento de activos y riesgos.
- La solución debe contar con una patente para la identificación pasiva de vulnerabilidades.
- La solución, mediante el monitoreo pasivo, deberá poder rastrear qué sistemas se comunican con qué puertos específicos, así como detectar cuando nuevos equipos se agreguen a la red.
- La solución permitir ver información detallada sobre la funcionalidad para solucionar problemas de actividad inusual del sistema o del usuario.

- La solución deberá poder desplegar el número de escáneres, monitores de red y agentes de escaneo donde sean necesarios sin que esto represente un incremento en costo para la institución.

- La solución deberá poder equilibrar cargas a través de múltiples escáneres de forma dinámica con base en la disponibilidad de cada escáner desplegado.

- Con el objetivo de no afectar activos de la institución, la solución solicitada deberá incluir la posibilidad de programar ventanas de escaneo.
- Poder generar reportes en diferentes formatos: PDF, RTF, CSV.

- La solución debe apoyar exploración IPv6**,** con el descubrimiento pasivo de objetivos utilizando IPv6.

- La solución debe poder realizar escaneos sin necesidad de instalación de agentes.

- La solución debe proporciona visibilidad de la superficie de ataque para gestionar y medir el riesgo cibernético. Debe proporcionar información priorizada de las vulnerabilidades con el mayor impacto y reducir los tiempos de identificar que una vulnerabilidad sea explotable en el corto tiempo.

- Poder clasificar por activos por grupos en función de las necesidades de la organización para poder categorizar los resultados y asignar las tareas correspondientes.

- La solución debe permitir a los administradores definir nuevos roles basados en funciones de trabajo y los niveles adecuados de acceso a la funcionalidad.

- La solución deberá contar con una gestión centralizada de credenciales para escaneo, permitiendo a un analista escanear equipos remotos sin conocer las credenciales del host.

- La solución debe soportar un número ilimitado de credenciales para usar para SSH, Windows y de Bases de Datos.

- La solución deberá poder iniciar automáticamente los servicios de registro remoto en los sistemas Windows cuando ejecuta un análisis con credenciales, luego automáticamente los detendrá una vez finalizada la exploración.

- Contar con un módulo que permita la creación de filtros para mejorar las búsquedas. Estos filtros deberán poder ser por lo menos protocolo, IP, vulnerabilidad, identificador CVE, CVSS, explotabilidad, vulnerabilidades en las noticias.

- La solución debe basarse en un análisis mediante combinación datos de inteligencia de amenazas de múltiples fuentes, análisis a través de un algoritmo de ciencia de datos que utiliza el aprendizaje automático para proporcionar la probabilidad de que una vulnerabilidad sea aprovechada por los factores de amenazas.

- Deberá contar con un API que permita hacer integraciones programáticas y con otras soluciones para intercambio de información.

- La solución debe permitir escaneos autenticados y sin autenticación.

- Los dashboards deberán poder mostrar la tendencia de identificación de vulnerabilidades y su evolución con el paso del tiempo, marcando tendencias y mostrando la información relevante de las vulnerabilidades.
- Los dashboards deberán permitir filtros a aplicar en función de los grupos de activos de la organización.

- Debe contar con la capacidad para identificar vulnerabilidades en dispositivos móviles (como iOS, Android, Windows).

- La solución deberá permitir la medición continua de la efectividad de las políticas definidas por la organización basados en objetivos de alto nivel que permitan identificar brechas a atender, mediante un conjunto de criterios que deben cumplirse en su conjunto.

- La solución deberá poder realizar un análisis posterior a una vulnerabilidad para validar si ya ha sido remediada, para poder marcar la vulnerabilidad como mitigada.
- La solución debe proporcionar información de capacidad de explotación contra las plataformas de validación, por lo menos Metasploit, CoreImpact o Canvas.

- Deberá realizar escaneo de vulnerabilidades de sistemas operativos, dispositivos de red, dispositivos de seguridad, firewalls de siguiente generación, hipervisores, bases de datos, servidores Web e infraestructuras esenciales para las vulnerabilidades, las amenazas y las infracciones de cumplimiento.

- La solución debe proporcionar auditoría de parches y configuraciones para los siguientes tipos de sistemas:
    - Windows y componentes de Microsoft: IIS, Exchange, Office, Explorer
    - UNIX / Linux
    - Check Point
    - Cisco
    - Palo Alto
    - Juniper
    - Fortinet
    - FireEye
    - Watchguard
    - OpenStack
    - HP Procurve
    - Extreme Networks
    - Huawei VRP
    - Blue Coat
    - Brocade

- Citrix
- NetApp
- VMWare vCenter/vSphere
- MongoDB

- La solución deberá permitir una clasificación dinámica de activos basados en criterios específicos definidos por los administradores.

- La solución debe proporcionar una integración con los sistemas de administración de parches, auditoría e informes de diferencias en los parches contra equipos valorados. Por lo menos se deben soportar: Microsoft WSUS/SCCM, Red Hat Satellite, IBM Tivoli Endpoint Manager, Symantec Altiris, Dell KACE K1000.

- La solución debe permitir a un usuario aceptar el riesgo (excepciones), permitiendo reconfigurar el nivel de riesgo a uno que sea lo que el administrador requiera.

- La solución deberá poder generar grupos de manera dinámica con base en la identificación de los activos y las condiciones establecidas.

- La solución debe proveer la respuesta del activo escaneado en cada prueba, pudiendo identificar que tiene el elemento evaluado.

- La solución debe poder evaluar equipos contra definiciones de SCAP y OVAL.

- La solución debe ser capaz de proporcionar información de reputación en procesos encontrados y la amenaza en inteligencia alimentada en busca de malware y botnets durante el análisis.
    - La solución deberá poder configurar reglas de escaneo con soporte de reglas YARA.

- Deberá permitir realizar auditorías basadas en las mejores prácticas y marcos de trabajo tales como: CERT, CIS, DISA STIG, PCI, FISMA.

- La solución deberá poderse integrar con el Directorio Activo para efectos de autenticación en el sistema.

- La solución deberá permitir construir flujos y alertas para los administradores para tomar acción vía email, tickets, o acciones automatizadas.

- La información de colección de eventos deberá poder ser mostrada en los dashboards de la consola.

- La solución de colección de eventos deberá poder contar con agentes ligeros para poder colectar la información.

- Un dispositivo virtual (Virtual Appliance) debe estar disponible para los motores de análisis y consolas, sin ningún tipo de costo adicional por distribución.

- Un servicio opcional de escaneo alojado externamente que es ASV PCI debe estar disponible para la digitalización de las redes perimetrales.

- El producto debe ser compatible con varios motores de análisis distribuidos geográficamente o lógicamente gestionados por una consola centralizada.

- El producto debe ser compatible con el equilibrio de carga y conmutación por error (load balance y fault tolerance) a través de múltiples escáneres de forma dinámica mediante la distribución de la carga entre los escáneres de exploración en base a la disponibilidad de escáner a través de todo el trabajo de exploración. Describir la estrategia de equilibrio de carga utilizada por el producto.

- El producto debe proporcionar licencias flexibles de despliegue del escáner con la capacidad de implementar escáneres adicionales sin costo adicional por sensor.

- El producto debe ofrecer la posibilidad de configurar los puertos, protocolos y servicios para las conexiones con escáneres desplegados en toda la red. Así permitiendo utilización de medios alternos de autenticación entre la consola central y el sensor.

- El producto debe ser configurable para permitir la exploración de estrangulación para evitar la generación de tráfico suficiente para interrumpir la infraestructura de red normal o reducir impacto en el ancho de banda.

- El producto debe proporcionar la capacidad de soportar línea de exploración (manual import) y los resultados que importan en el servidor por sensores no manejados.

- El producto debe permitir la entrada y el almacenamiento seguro de credenciales de usuario, incluyendo las cuentas locales y de dominio de Windows, Unix y su y sudo a través de ssh. Detalle el método utilizado para cifrar estos datos.

- El producto debe proporcionar la capacidad de elevación de privilegios contra objetivos de los usuarios normales a raíz de acceso / administrativa. Debe apoyar SUDO, SU o una combinación de estos.

- El producto debe soportar un número ilimitado de credenciales “ssh”.

- El producto debe integrarse con cofres digitales de credenciales como CyberArk para la utilización y administración de credenciales.

- El producto debe ser compatible con un descubrimiento activos, capaz de que no ocupe contra el consumo de licencias adquiridas. Detalle a política de escáner que cumpla.

- El producto debe proporcionar una capacidad de exploración activa y capacidad de análisis de red pasiva para el descubrimiento de activos.

- El producto debe ser capaz de detectar dispositivos móviles. Dispositivos especializados como controles industriales y IoT.
- El producto no debe depender de ningún producto o partes de un tercero para el descubrimiento de activos, escaneo de puertos, o la identificación del sistema operativo. Debe estar nativamente integrado a la consola de gestión central.
- El producto debe proporcionar escaneo de aplicaciones de web integrado y descubrimiento de servicios de base de datos.
- El producto debe ser capaz de detectar los servicios que se ejecutan en puertos no estándar.
- El producto debe ser capaz de detectar servicios configurados para no mostrar "banners" de conexión.
- El producto debe ser capaz de probar varias instancias del mismo servicio que se ejecuta en diferentes puertos.
- El producto debe ser capaz de escanear anfitriones muertos (dispositivos que no responden a un ping)
- El producto debe apoyarse del uso opcional del comando netstat para la enumeración rápida y precisa de los puertos abiertos en un sistema cuando se suministran credenciales.
- El producto debe ser compatible con el uso de SMB y WMI para la digitalización de los sistemas Windows.
- El producto debe ser capaz de iniciar automáticamente los servicios de registro remoto en los sistemas Windows cuando ejecuta un análisis con credenciales, luego automáticamente se detendrían los servicios de nuevo una vez finalizada la exploración.
- El escáner debe ser compatible con Secure Shell (SSH) con la capacidad de escalar privilegios de análisis de vulnerabilidad y auditorías de configuración en sistemas Unix.
- El producto debe proporcionar la capacidad de sintonizar políticas de análisis de impacto mínimo en las redes y los objetivos.
- El producto debe proporcionar descubrimiento activo y pasivo de puntos de acceso inalámbrico (WAP).
- El producto debe proporcionar la capacidad de detectar nuevos dispositivos y enviar alertas vi las notificaciones de correo electrónico, registro del sistema, o la consola.
- El producto debe proporcionar la capacidad para poner en marcha de forma automática exploraciones contra nuevos dispositivos.

- El producto debe respaldar el uso de un agente soluble para la auditoría.

ESCANEADO DE VULNERABILIDAD

- El producto debe ser capaz de basado en agente y las pruebas sin agente tanto para la detección de la vulnerabilidad local y remota sin la necesidad de un agente de cliente instalado en el dispositivo de destino.
- El producto debe proporcionar una cantidad significativa de comprobaciones de vulnerabilidad más allá del sistema operativo o plataforma Microsoft Windows.
- El producto debe ser capaz de **seguir** los cambios **de DHCP** mediante la asociación de los resultados del análisis con los nombres de host del sistema.
- El producto debe ser compatible con la capacidad de preservar los resultados del análisis de **los sistemas inactivos** por un período personalizable y de Identificación de las vulnerabilidades en el tiempo
- El producto debe incluir salida detallada de los resultados de exploración para incluir información tal como **versiones de librerías DLL o ejecutables** esperados y los encontrados.
- El producto debe ser compatible o aprobado por **CVE** y proporcionar por lo menos 10 años de cobertura del estándar de CVE.
- El producto debe informar sobre **las debilidades conocidas** en un objetivo dado, identificado por las organizaciones de asesoramiento de seguridad (por ejemplo, Vulnerabilidades y Exposiciones Comunes base de datos (CVE) o la base de datos de Open Source vulnerabilidad (OSVDB) o la Security Focus Bugtraq (BID) o cualquier combinación de ellos).
- El producto debe apoyar la capacidad de agregar opcionalmente el servicio **reporte PCI Aproved Scanning Vendor (ASV)** para las revisiones trimestrales.
- El producto debe ser compatible con el escaneo de vulnerabilidades **PCI DSS Compliance.** El producto debe incluir plantillas de escaneo para PCI y PCI DSS predefinidas que cumplan con los criterios actuales de PCI DSS para escaneo en red. Debe existir funcionalidad para filtrar todas las vulnerabilidades relevantes que no sean PCI.
- El producto debe proporcionar **auditoría de parches para los sistemas operativos de Microsoft y aplicaciones,** como Windows XP, Windows 7, Windows 2008, Windows 2012, Internet Explorer, Microsoft Office, IIS, Exchange, y otros más.

- El producto debe proporcionar **auditoría de parches para los principales sistemas operativos Unix** a incluir Mac OS, Linux, Solaris, IBM AIX, HP-UX, y otros más.
- El producto debe proporcionar **revisión de parches para la infraestructura de red** para incluir Cisco, Palo-Alto, Juniper y más. Lista de la infraestructura de red disponible para la auditoría de parches.
- El producto debe apoyar la exploración de **SCADA** y otros dispositivos integrados o controles industriales por vulnerabilidad o cumplimiento con mejores prácticas.
- El producto debe dar cobertura a **aplicaciones de terceros** como Java y Adobe y otros.
- El producto debe proporcionar una integración con **los sistemas de administración de parches** para la auditoría e informes de parches delta en los resultados de digitalización, a incluir Microsoft WSUS / SCCM, Redhat Satelite, IBM Tivoli Endpoint Manager, Altiris, VMware Go.
- El producto debe proporcionar una integración con los **directores de dispositivos móviles (MDM)** para el descubrimiento de dispositivo móvil y su auditoría de riesgo.
- El producto debe proporcionar capacidades de auditoría para **dispositivos** y redes de control industrial o **SCADA.**
- El producto debe ser capaz de escanear **Amazon Web Services** y Amazon Machine Images.
- El fabricante del producto debe incluir un agente para el **Amazon Web Services** Linux y otro Amazon Machine Images.
- El producto debe proporcionar información de reputación en procesos encontrados y la amenaza en inteligencia alimentada en busca **de malware y botnets** durante el análisis.
- El producto debe proveer la puntuación de vulnerabilidad de acuerdo con el estándar de la industria aceptado, es decir, el Common Vulnerability Scoring System **(CVSS).**
- El producto debe proporcionar mecanismo **de puntuación ponderada** personalizable basado en estándares de la industria aceptado como CVSS.
- producto debe proporcionar **información de explotabilidad** contra las plataformas de validación como Metasploit, Canvas, y otras.
- El producto debe proporcionar información de **explotabilidad por malware.**
- El producto debe **inteligentemente seleccionar pruebas** basadas en la información obtenida de los análisis iniciales para intentar más pruebas sobre la base de la información obtenida previamente sobre un dispositivo o equipo dado. Por ejemplo, basado en el sistema operativo.

- El producto debe **realizar el seguimiento del ciclo** de **vida** de las instancias de vulnerabilidad en que se refiere a los hosts individuales, así como el medio ambiente, para incluir cuando una vulnerabilidad fue descubierta, ultima ves observada, y mitigado o previamente-mitigado.

- El producto debe ser compatible con la vulnerabilidad y el cumplimiento en exploración de **servidores VMWare** utilizando el API de VMware nativo.

- El producto debe permitir **la detección programada** de dispositivos.

- El producto debe permitir que las pruebas seleccionadas se activen o deshabiliten durante las exploraciones.

- El producto debe incluir la capacidad de desactivar los controles potencialmente dañinos de modo que sean opcionales.

- El producto debe **iniciar** y detener las búsquedas en el calendario sin interacción con el usuario **de forma automática**

- El producto debe permitir la posibilidad de **pausar y reanudar** las exploraciones de forma interactiva.

- El producto debe permitir que las exploraciones que no se completen dentro de un período de tiempo establecido se trasladen al siguiente período programado.

- El producto debe ser capaz de aceptar **objetos de análisis** en múltiples formatos, incluyendo los nombres DNS, rangos de IP y clases de IP, y las listas de activos predefinidos. Por ejemplo 10.0.1.1 - 10.0.1.100. También debe admitirse la importación de una lista de IP contenidas en un archivo fuente. Describa la forma en que los objetivos pueden introducirse en el producto.

- El producto debe apoyar exploración **IPv6,** con el descubrimiento pasivo de objetivos utilizando IPv6.

- El producto debe proporcionar la capacidad de excluir el escaneo de dispositivos periféricos como las impresoras o sistemas “embeded”.

- El producto debe proporcionar la detección de la vulnerabilidad para **Novell Netware.**

AUDITORÍA DE CUMPLIMIENTO

- El producto debe ser capaz de basada en agentes y sin agentes la auditoría de cumplimiento con controles de seguridad y mejores prácticas.

- El producto debe tener la funcionalidad “opcional” de monitoreo por medio de un agente o cliente instalado en el dispositivo de destino.

- El producto debe proporcionar una vista consolidada de todos los resultados de auditoría de vulnerabilidad y cumplimiento. Con paneles de control o Dashboards sugeridos, y la capacidad de crear nuevos detalladamente.

- El producto debe proporcionar puntos de referencia de seguridad y auditoría de configuración para el cumplimiento de las normas reguladoras como PCI y otras industrias y proveedores estándares de mejores prácticas como CIS o NIST. Enumere los puntos de referencia admitidos.

- El producto debe proporcionar puntos de referencia de seguridad y auditoría de configuración para las mejores prácticas de proveedores o fabricantes como Microsoft, Cisco, PaloAlto y VMware.

- El producto debe proporcionar auditoría de VMWare ESXi y vCenter utilizando el SOAP API propio de VMware.

- El producto debe proporcionar verificación de los sistemas operativos de Microsoft para la configuración de seguridad y configuraciones. Enumere los proveedores y las versiones del sistema operativo compatibles con puntos de referencia disponibles.

- El producto debe proporcionar la auditoría de los principales sistemas operativos Unix / Linux para la configuración de seguridad y configuración de aplicativos instalados. Enumere los proveedores y las versiones del sistema operativo compatibles con puntos de referencia disponibles.

- El producto debe proporcionar auditoria de bases de datos para la configuración de seguridad y configuraciones. Enumere los proveedores de bases de datos y las versiones compatibles con los puntos de referencia disponibles.

- El producto debe proporcionar auditoria de aplicaciones para la configuración de seguridad y configuración. Enumere los proveedores de aplicaciones y las versiones compatibles con puntos de referencia disponibles.

- El producto debe proporcionar auditoria de infraestructura de red o equipos de comunicaciones, para su endurecimiento de seguridad y prácticas recomendadas de configuración. Enumere los proveedores de la infraestructura de red y las versiones compatibles con puntos de referencia disponibles.

- El producto debe proporcionar auditoria de paquetes antivirus específicos por: instalación, últimas actualizaciones y el estado de arranque del producto. Enumere los paquetes antivirus y las versiones compatibles con puntos de referencia disponibles.

- El producto debe proporcionar verificación de la información de identificación personal (PII) y otros contenidos sensibles o sensitivos. Enumere los puntos de referencia de auditoría de contenido disponibles.

- El producto debe permitir que las plantillas utilizadas con políticas de auditoría puedan ser personalizables según las necesidades específicas de la organización. Donde se puedan definir controles internos para sistemas de TI.

- El producto debe proporcionar puntos de referencia certificados de la CEI.

- El producto debe ser validado para NIST SCAP 1,2.

- El producto debe ser capaz de ejecutar auditorías de cumplimiento de los controles mencionados en los DISA STIG del Departamento de Defensa.

FLUJO DE DATOS O TRABAJO (WorkFlow)

- El producto debe facilitar la automatización completa de escaneo, informes y alertas.

- El producto debe proporcionar vistas separadas para vulnerabilidades activas, pasivamente descubiertas, asociadas a cumplimiento y riesgo en dispositivos móviles.

- El descubrimiento de dispositivos móviles, no debe depender de agentes instalados en los dispositivos, ni en sistemas de gestión como los MDM.

- El producto debe agregar los resultados de las exploraciones individuales en vistas de vulnerabilidad acumulativos con el filtrado y análisis para permitir capacidades de desglose y pivote.

- El producto debe tener vistas separadas de vulnerabilidades activas y mitigadas con la migración automática de vulnerabilidades de activo a mitigado una vez un análisis determina que la vulnerabilidad ya no está presente.

- El producto debe tener la capacidad para marcar una vulnerabilidad por haber sido mitigado con anterioridad, pero que ha aparecido de nuevo como podría ocurrir cuando un sistema se restaura a partir de copia de seguridad o una vieja copia de una máquina virtual se vuelve a conectar.

- El producto debe proporcionar un filtro amplio de los resultados de vulnerabilidad agregada con capacidades de desglose. Entre estos se puede considerar si la vulnerabilidad es fácil de

comprometer, o si está presente un “exploit”, en herramientas para hacer pruebas de validación.

- El producto debe proporcionar análisis de la ruta de ataque.
- El producto debe proporcionar vistas de remediación que se priorizan y sean simplificadas para la audiencia de forma automática.
- El producto debe proporcionar la posibilidad a los usuarios autorizados a ejecutar exploraciones de remediación individuales para verificar vulnerabilidades se han abordado correctamente.
- El producto debe proporcionar la capacidad de automáticamente agrupar objetivos, utilizando los resultados del análisis para generar listas de activos dinámicas.
- El producto debe permitir a un usuario a aceptar el riesgo (hacer una excepción) con fechas de caducidad configurables por una vulnerabilidad detectada, o a la refundición de riesgo (cambiar los niveles de gravedad) a un nivel que no sea lo que el vendedor ha definido para que dicha vulnerabilidad.
- El producto debe proporcionar funcionalidad de tickets de remediación integrada, que también puede enviar entradas a los sistemas de 3ª partes u otros fabricantes.
- El producto debe ser compatible con la asignación de tickets a los usuarios individualmente.
- El producto debe proporcionar capacidades de alerta activada por vulnerabilidades y eventos en diferentes sistemas de infraestructura.
- El producto debe admitir la definición de alertas basadas en el análisis de vulnerabilidades o los resultados de la auditoría de configuración.
- Las acciones de alerta deben incluir: correo electrónico personalizable con contexto que utilice variables específicas, creación y asignación de un ticket, inicio de un escaneo, generación de un evento syslog y generación automática de informes o reportes.

REPORTES / INFORMES

- El producto debe ser compatible con la generación de informes o reportes personalizadles ya sea utilizando plantillas suministradas por el vendedor o sin plantillas.
- El producto debe proporcionar la capacidad de filtrar los resultados en la presentación de informes por una variedad de criterios para incluir listas de o grupos de activos, repositorios, direcciones de IP, tipos de vulnerabilidad, texto sin formato, y los campos de fechas.

- El producto debe proporcionar informes integrados de exploración, análisis de configuración, y de registros.

- El producto debe proporcionar, en la capacidad de la presentación de informes, automatizar completamente para incluir la ejecución programada y la entrega de informe posterior a la exploración.

- El producto debe proporcionar la capacidad de producir informes ad-hoc durante la visualización de los resultados en la consola. Las exportaciones de PDF y CSV estarán disponibles.

- El producto debe ser compatible con la capacidad de producir informes en los siguientes formatos de reporte: PDF, CSV, XML

- El producto debe proporcionar tendencias adaptables de los resultados del análisis en informes con resultados filtrados para definir múltiples líneas de tendencia en un solo componente gráfico.

- El producto debe proporcionar tablas de matriz que resumen los números a través de muchos conjuntos filtradas de resultados.

- El producto debe proporcionar una alimentación automatizada de informes de plantillas para los temas de seguridad y cumplimiento.

- El producto debe proporcionar los informes de cumplimiento normativo, sin costo adicional. Esto a incluir CIS, ISO2700, y PCI DSS entre otros.

- Los informes deben tener la posibilidad de incluir los nombres de host (NetBIOS, DNS), junto con las direcciones IP como mínimo.

- El producto debe proporcionar la capacidad de cifrar y proteger con contraseña los informes generados de manera automática, antes de ser enviados por correo electrónico.

- El producto debe proporcionar la capacidad de correo electrónico de forma automática para reportes.

- El producto debe proporcionar la capacidad de empujar informes que utilizan los servicios de publicación web.

- El producto debe permitir importación de imágenes personalizadas para ser incluidas en la personalización de reportes.

PANELES - DASHBOARDS

- El producto debe proporcionar calificaciones de alto nivel que muestre la madures de las métricas de seguridad y cumplimiento.

- El producto debe incluir elementos gráficos y paneles de control personalizables, listos para la visualización de las vulnerabilidades y el estado del entorno evaluado.
- El producto debe proporcionar tendencias adaptables de los resultados del análisis en cuadros de mando, utilizando resultados filtrados para definir múltiples líneas de tendencia en un solo componente gráfico.
- El producto debe permitir que cada usuario defina en su perfil, múltiples cuadros de mando específicos del usuario.
- Elementos del tablero de instrumentos deben ser totalmente personalizables mediante el filtrado, para mostrar los datos en base a la lista de activos, vulnerabilidad o de control de la conformidad, el tiempo, la palabra clave de búsqueda, dirección IP, etc.
- Los cuadros de mando de actualización de los datos deben ser configurable para actualizar en forma programada y ad-hoc.
- El producto debe proporcionar la capacidad de importar / exportar las plantillas y presentación de informes.
- El producto debe proporcionar la capacidad de compartir las plantillas y presentación de informes con otros usuarios de la misma empresa.
- El producto debe proporcionar la capacidad para definir varios elementos visuales para paneles personalizados a incluir gráficos “pie charts”, gráficos de barras, matriz, y de tendencias.
- El producto debe incluir un catálogo con paneles o Dashboards que se presenten como plantillas ejemplo, y que sean alineadas en torno a diferentes audiencias, normas de cumplimiento y los controles de seguridad.
- El producto debe adaptarse a las opciones de diseño y formato personalizables para paneles o Dashboards.

4. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- El proveedor debe suplir las certificaciones de la industria de la solución.
- El proveedor debe diseñar y presentar para su aprobación un plan de trabajo, detalle de la metodología a utilizar y cronograma.
- El proveedor debe proporcionar entrenamiento de la solución.
- El proveedor debe implementar la herramienta de escaneo de vulnerabilidades de la institución una vez sea revisado y aprobado por el personal de la SIB.
- El suplidor debe tener una solución de hardware dedicada para satisfacer todos los requisitos del cliente.
- El suplidor debe proporcionar una configuración de hardware recomendada basada en los criterios de tráfico real y aplicaciones de seguridad de próxima generación proporcionadas por el cliente.
- El proveedor debe ofrecer 20 horas de entrenamiento de curso oficial aprobado por el fabricante del producto, para al menos 3 personas.

5. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- Propuesta de plataforma de herramienta de escaneo de vulnerabilidades
- Plan de trabajo de Implementación de herramienta de vulnerabilidades
- Plataforma de escaneo de vulnerabilidades de la Superintendencia de Bancos en funcionamiento
- Documento de cierre de proyecto que contenga las configuraciones y pasos realizados durante la implementación del producto.

6. PERFIL PROFESIONAL

- El proveedor de la herramienta de vulnerabilidades debe tener al menos 5 años de experiencia en el mercado de seguridad y proporcionar referencias sobre proyectos exitosos en clientes.
- El proveedor debe proporcionar evidencia de liderazgo año tras año en herramienta para escaneo de vulnerabilidades para empresa, independientes de la seguridad de la industria.
- El ingeniero para la instalación, configuración, pruebas y puesta en funcionamiento de la solución en sitio deberá contar con certificación del manejo de la herramienta de escaneo de vulnerabilidades.

3. DESKTOP CENTRAL ENTEPRISE EDITION DE LA HERRAMIENTA MANAGEENGINE PARA LA ASISTENCIA REMOTA A USUARIOS FINALES

Objetivo

Adquisición e implementación de módulo Desktop Central para la plataforma MangeEngine para la administración de escritorios de Windows y asistencia técnica remota a usuarios finales para uso de la Superintendencia de Bancos

ITEM	DESCRIPCION	UNIDAD	CANTIDAD
1	ManageEngine Desktop Central Enterprise (Distributed) Edition Licenciamiento perpetuo para 1000 computadoras y 1 usuario técnico	UN	1
2	Mantenimiento Anual para Desktop Central Enterprise (distributed) para 1000 Computadoras y 1 usuario técnico	UN	1
3	ManageEngine Desktop Central Addons – Perpetual Licensing Model - Paquete para 10 usuarios adicionales	UN	1
4	Licenciamiento del paquete Multi-Language (Idioma Español)	UN	1
5	Mantenimiento Anual para el paquete Multi-Language (Idioma Español)	UN	1
6	Servicios Técnicos Profesionales - Instalación, Configuración, Puesta en marcha, transferencia de conocimiento, soporte local 9*6 durante 12 meses.	UN	1

4. ROBUSTECIMIENTO DE LA PLATAFORMA CITRIX NETSCALER

1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente la Superintendencia de Bancos (SIB) tiene implementado un appliance virtual Citrix NetScaler ADC, los nuevos desarrollos de aplicaciones tanto internas como externas han sido más demandantes, por lo que se ha creado la necesidad de robustecer dicha plataforma con un ambiente físico en alta disponibilidad tanto en nuestro site principal como en nuestro site alterno.

2. OBJETIVOS

Hacer la plataforma más robusta escalable y estable, renovando y robusteciendo la plataforma de citrix NetScaler de la Superintendencia de Bancos

a. Objetivos Específicos

- Implementar nuevas medidas de alta disponibilidad para las aplicaciones internas y Externas.
- Responder en tiempos mínimos las conexiones y solicitudes de las entidades de intermediación financiera.
- Establecer un mecanismo de balanceo de cargas automatizado.
- Establecer controles de conexiones seguras.

3. FUNCIONALIDADES DE PLATAFORMA DE CITRIX NETSCALER

La solución debe consistir de los siguiente:

1. (4) ADCMPX8905ADVED.
2. (4) ADC PW SP 450W AC MOD 5900/8900/SDW2100.
3. (4) 3YRSGLDMNTADCMPX8905ADVED.
4. (4) ADC SFP GIGABIT ETHERNET LX – SGL.
5. (4) SD-WAN 210-50-SE (50 MB) SE APPL.
6. (4) 3YRSGLDMNTSD-WAN210-50-SE (50MB) SEAPPL.
7. (1) SD-WAN 1100-500 SE APPL.
8. (1) 3 YR GLD MTCE SD-WAN 1100-500 SE.
9. (1) SD-WAN 1100-500 SE COLD SPARE APPL.
10. (1) SERVICIOS PROFESIONALES E INSTALACIÓN

REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Esta solución debe ser suplida y manejada exclusivamente por el proveedor.

- El proveedor debe proporcionar entrenamiento formal de la solución.

- El proveedor debe diseñar y presentar para su aprobación un plan de trabajo, detalle de la metodología a utilizar y cronograma.

- El proveedor debe implementar la solución para las necesidades de la SIB

PERFIL PROFESIONAL

- El proveedor de la solución debe tener al menos 5 años de experiencia en el mercado y proporcionar referencias sobre proyectos exitosos en clientes.

- El proveedor debe de personal certificado en la solución

- El proveedor debe ser capaz de atender todo el alcance de los requisitos de la solución, incluido el rendimiento y también velocidad de conexión.

5. DISPOSITIVOS PARA LA REDUNDANCIA DE LA CONECTIVIDAD DE LAS REDES DE DATOS ENTRE LOS DIFERENTES NIVELES

1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente la Superintendencia de Bancos (SIB) tiene implementado en sus diferentes niveles equipos de las redes de datos de alta tecnología, en ese mismo sentido, es muy importante que estos equipos estén conectados de una manera confiable, segura y redundante.

2. OBJETIVOS

Mantener los equipos de las redes de datos conectados de manera adecuada, segura y redundante en los diferentes niveles de la Superintendencia de Bancos.

a. Objetivos Específicos

Implementar nuevas medidas de alta disponibilidad para la conectividad de las redes de datos en los diferentes niveles.

3. FUNCIONALIDADES DE PLATAFORMA

La solución debe consistir de los siguiente:

1. (60) Cisco Glc-sx-mmd 10-2626-01 1000base SX SFP Transceiver Module
    a) Version 2007 o Superior.

6. RACK PDU MONITOREABLES

1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente la Superintendencia de Bancos (SIB) tiene implementado en sus centros de datos equipos de alta tecnología, en ese mismo sentido, es muy importantes que estos equipos estén conectados a una alimentación eléctrica confiable, segura y redundante.

2. OBJETIVOS

Mantener los equipos con una alimentación eléctrica adecuada, segura y redúndate en los centros de datos de la Superintendencia de Bancos

2.1 Objetivos Específicos

- Implementar nuevas medidas de alta disponibilidad para la alimentación eléctrica de los equipos en los centros de datos.

3. FUNCIONALIDADES DE PLATAFORMA

La solución debe consistir de los siguiente:

1. (8) RACK PDU 2G, METERED, ZERO, 30A, 200/208V,
    a. (36) C13
    b. (6) C19
    c. Input Connections NEMA L6-30P
    d. (2) Años de Garantía en piezas y servicios

7. RENOVACION CENTRAL TELEFONICA (CISCO CUCM)

1. PLANTEAMIENTO DE LA NECESIDAD

La Superintendencia de Bancos requiere la renovación de su plataforma de central telefónica, la misma es renovada anualmente para mantener el nivel de soporte y garantía adecuado para solventar cualquier incidente que esta requiera, así como también de las sustituciones físicas de los diferentes componentes que esta conforma.

2. DESCRIPCIÓN DE LOS BIENES Y ESPECIFICACIONES TÉCNICAS

Se requiere la renovación de los diferentes componentes detallados a continuación.

Cisco Unified SIP Phone 3905, Charcoal, Standard Handset	18
Cisco UC Phone 7841	152
Cisco UC Phone 7861	5
Cisco UC Phone 7821	194
Cisco Unified Phone 8945, Phantom Grey, Standard Handset	30
Cisco Business Edition 6000-Electronic SW Delivery-Top Level	1
SX20 Quick Set HD, NPP, 4x PHDCam, 1 mic, remote cntrl	1
SX20 Codec - encrypted	1
BE6K Starter Pack - Single Fulfillment Enforcement	1
Business Edition 6000 v10 export restricted software	1
Cisco Business Edition 6000 - Essential User Connect License	20
BE6K UCM 10X Basic User Connect License - Single Fulfillment	195
Cisco Business Edition 6000 - Basic User Connect License	195
Cisco Business Edition 6000- Voicemail/Unified Messaging UCL	160
Cisco Business Edition 6K Upg - PAK - Partial Fulfillment	1
Cisco Business Edition 6000 - Enhanced User Connect License	160
BE6K UCM 10X Enhanced User Connect License - Single	185
BE6000 UCM 10X Telepresence Room User Connect License	1

3. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Esta solución debe ser suplida y manejada exclusivamente por el proveedor.
- El proveedor debe implementar la solución para las necesidades de la SIB

4. PERFIL PROFESIONAL

- El proveedor de la solución debe tener al menos 5 años de experiencia en el mercado y proporcionar referencias sobre proyectos exitosos en clientes.
- El proveedor debe de personal certificado en la solución
- El proveedor debe ser capaz de atender todo el alcance de los requisitos de la solución, incluido el rendimiento y también velocidad de conexión.

8. RENOVACION SOPORTE PLATAFORMA HPE

1. PLANTEAMIENTO DE LA NECESIDAD

La Superintendencia de Bancos requiere la renovación de su plataforma HPE, la misma es renovada anualmente para mantener el nivel de soporte y garantía adecuado para solventar cualquier incidente que esta requiera, así como también de las sustituciones físicas de los diferentes componentes que esta conforma.

2. DESCRIPCIÓN DE LOS BIENES Y ESPECIFICACIONES TÉCNICAS

Se requiere la renovación de los diferentes componentes detallados a continuación.

HPE Foundation Care 24x7 SVC
HPE Hardware Maintenance Onsite Support
Hardware Problem Diagnosis
Onsite Support
Parts and Material provided
4 Hr Onsite Response
24 Hrs Std Office Days
24 hrs, Day 6
24 hrs, Day 7
Holidays Covered

Seriales:

USE337E39E
USE337E39H
USE337E39J
2M233009R8
2M2112008Z
USE1179SYL
USE1179T0X
USE1179T33

3. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Esta solución debe ser suplida y manejada exclusivamente por el proveedor.
- El proveedor debe implementar la solución para las necesidades de la SIB

4. PERFIL PROFESIONAL

- El proveedor de la solución debe tener al menos 5 años de experiencia en el mercado y proporcionar referencias sobre proyectos exitosos en clientes.
- El proveedor debe de personal certificado en la solución
- El proveedor debe ser capaz de atender todo el alcance de los requisitos de la solución, incluido el rendimiento y también velocidad de conexión.

2.9 Duración del Suministro

La Convocatoria a Licitación se hace sobre la base de un suministro para un período **según cuadro 2.8 Descripción de los Bienes** contados a partir de **la fecha de adjudicación** 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 dentro del ámbito territorial de la República Dominicana y conforme al Cronograma de Entrega establecido. En caso de no especificarse, **todos los bienes y servicios serán entregados en la sede principal de La Superintendencia de Bancos de la Republica Dominicana, Ave. México esq. Leopoldo Navarro, no. 52, Gazcue.**

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) (RNC)
Firma del Representante Legal
COMITÉ DE LICITACIONES
Superintendencia de Bancos de la República Dominicana
Referencia: SIB-LPN-002/2019
Dirección: Av. México #52, Esq. Leopoldo Navarro, Gazcue, Santo Domingo, R.D.
Teléfonos: 809-685-8141 ext. 276
Correo: wsolis@sib.gob.do

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 de Conferencias de la Superintendencia de Bancos de la Republica Dominicana, ubicado en el 2do Nivel**, sito **Ave. México no. 52 esq. Leopoldo Navarro, Gazcue** desde las **10:00 am** de los días indicado en el Cronograma de la Licitación y sólo podrá postergarse por causas de Fuerza Mayor o Caso Fortuito definidos en el presente Pliego de Condiciones Específicas. A partir de las 10:00 am no se recibirán más ofertas.

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", y Muestras

Los documentos contenidos en el **"Sobre A"** deberán ser presentados en original debidamente marcado como "**ORIGINA**L" en la primera página del ejemplar, junto con **Dos (2)** fotocopias simples de los mismos, debidamente marcada, en su primera página, como "**COPIA**". El original y las copias deberán firmarse en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía. **Deberán presentarse en carpetas de 3 hoyos tipo D, sin grapas, debidamente identificada y separadas por separadores que indiquen cada documento requerido según el punto 2.14 Documentos a Presentar, tanto el original como la copia.**

Conjuntamente con la entrega del "**Sobre A",** los Oferentes/Proponentes deberán hacer entrega de las muestras de los productos de acuerdo al procedimiento establecido en el numeral 2.15, del presente Pliego de Condiciones Específicas. Deberán presentar el **Formulario de Entrega de Muestras**, que deberá estar contenido en el **"Sobre A"** en Un **(1) Original** y **Dos (2) fotocopias** simples. El original y la copia deberán firmarse en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía.

No se considerarán válidas las Ofertas Técnicas de aquellos productos de los que no se hayan recibido las muestras correspondientes,

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

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social) (RNC)

Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
SUPERINTENDENCIA DE BANCOS DE LA REPÚBLICA DOMINICANA
PRESENTACIÓN: **OFERTA ECONÓMICA**
REFERENCIA: SIB-LPN-002/2019

2.14 Documentación a Presentar

A. Documentación Legal:

1. Formulario de Presentación de Oferta. **(SNCC.F.034)**
2. Formulario de Información sobre el Oferente **(SNCC.D.042).**
3. Constancia de Registro Nacional de Proveedores **(RNP)**, emitido por la Dirección General de Contrataciones Públicas (el nombre que aparezca en este registro debe ser consistente con los demás documentos presentados).
4. Certificación emitida por la Dirección General de Impuestos Internos **(DGII)**, donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones fiscales.
5. Certificación emitida por la Tesorería de la Seguridad Social **(TSS)**, donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones de la Seguridad Social.
6. Copia de los **Estatutos Sociales de la Empresa**
7. Copia del **Acta de Asamblea Constitutiva** (con su nómina de presencia)
8. Copia de la última **Acta de Asamblea vigente** que elige o ratifica la Directiva actual (con su nómina presencia)
9. En caso de que los estatutos hayan sufrido alguna modificación depositar el **Acta de Asamblea Extraordinaria** que conoce de dicha modificación.
10. **Lista de Suscriptores** Actualizada
11. Copia Certificado de **nombre comercial vigente**
12. Copia del **Certificado de Registro Mercantil vigente**
13. Copia del **Certificado de Registro Nacional de Contribuyentes vigente**
14. Copia de las **Certificaciones Vigentes** de que goce la empresa en el caso que tuviera alguna (s).

B. Documentación Financiera:

1. Copia de los **estados financieros** de los últimos dos años firmados y sellados por un CPA.

C. Documentación Técnica:

1. **Oferta Técnica**: Descripción de los bienes ofertados, tiempos de entrega y garantías.
2. Autorización del Fabricante **(SNCC.F.047):** Documentación que certifique que está debidamente autorizado por el fabricante o productor del caso para suministrar los bienes en cuestión en la República Dominicana.
3. Resumen de experiencia del Personal Profesional propuesto **(SNCC.D.045)**: Certificación de los técnicos.
4. Resumen de Experiencia del Oferente en Servicios Similares (de igual magnitud). **(SNCC.D.048)**
5. **Cronograma y Plan de Trabajo**.

2.15 Forma de Presentación de las Muestras de los Productos

Los Oferentes/Proponentes deberán entregar las muestras conjuntamente con su **"Sobre A"**, que contiene el Formulario de Entrega de Muestra**,** entregado por **Superintendencia de Bancos de la Republica Dominicana**, debidamente completado y firmado por el Representante Legal de la empresa, en un (1) original y dos (2) copias, escritos a máquina o computadora, para ser distribuidos de la siguiente manera:

- El original será conservado por el Equipo de Recepción de Muestras, designado al efecto.
- La primera copia, se adjuntará a la muestra correspondiente.
- La segunda copia será del Oferente/Proponente.
- La tercera copia para los fines que correspondan.

LA PRESENTACIÓN EN OTRO FORMATO INVÁLIDA LA OFERTA

Formulario de Entrega de Muestra **(SNCC.F.056)**.

La muestra se entregará físicamente y con sus especificaciones técnicas completas. En el punto 2.8 Descripción de los Bienes y Servicios especifica cuáles son las muestras que deberá entregar.

Una vez que se haya realizado la revisión de lugar, verificando que los datos que figuran en el Formulario se corresponden con las muestras y asentando una marca de cotejo en cada renglón revisado, el miembro del Comité de Recepción de Muestras correspondiente firmará y sellará como **"RECIBIDO"** el original y sus copias.

Todo Oferente/Proponente que no haya entregado las muestras requeridas será descalificado en el renglón que corresponda.

El apartado de observaciones en el indicado formulario será para uso exclusivo del técnico que reciba las muestras. En él se reflejarán las incidencias, si las hubiere en el momento de la recepción.

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

A) Formulario de Presentación de Oferta Económica (SNCC.F.033 – Modificado y anexo en el portal de Compras y Contrataciones), presentado en **Un (1)** original debidamente marcado como "**ORIGINAL**" en la primera página de la Oferta, junto con **(dos) 2** fotocopias simples de la misma, debidamente marcadas, en su primera página, como "**COPIA**". 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. Podrá presentarse una Garantía Bancaria o Póliza de fianza, por el monto equivalente al 1% del monto total proyectado para el servicio por el período correspondiente.

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

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social) (RNC)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
SUPERINTENDENCIA DE BANCOS DE LA REPÚBLICA DOMINICANA
PRESENTACIÓN: **OFERTA ECONÓMICA**
REFERENCIA: SIB-LPN-002/2019

Las Ofertas deberán ser presentadas únicas y exclusivamente en el formulario designado al efecto, **(SNCC.F.033 – Modificado y anexo en el portal de Compras y Contrataciones)**, y el cual estará debidamente sellado por la **Superintendencia de Bancos de la República Dominicana 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.

Ley 183-02 que aprueba la Ley Monetaria y Financiera

*"**Artículo 18. Naturaleza**. La Superintendencia de Bancos es una entidad pública de Derecho Público con personalidad jurídica propia. Tiene su domicilio en su oficina principal de Santo Domingo, Distrito Nacional, Capital de la República Dominicana, pudiendo establecer otras oficinas dentro del territorio nacional.*

La Superintendencia de Bancos está exenta de toda clase de impuestos, derechos, tasas o contribuciones, nacionales o municipales y en general, de toda carga contributiva que incida sobre sus bienes u operaciones. La Superintendencia de Bancos disfrutará, además, de franquicia postal y telegráfica. Contratará la adquisición de bienes y prestación de servicios necesarios para su funcionamiento con arreglo a los principios generales de la contratación pública y en especial de acuerdo a los principios de publicidad, concurrencia y transparencia, conforme Reglamento dictado por la Junta Monetaria."

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

A fin de cubrir las eventuales variaciones de la tasa de cambio del Dólar de los Estados Unidos de Norteamérica (US$), **Superintendencia de Bancos de la Republica Dominicana** podrá considerar eventuales ajustes, una vez que las variaciones registradas sobrepasen el **cinco por ciento (5%)** con relación al precio adjudicado o de última aplicación. La aplicación del ajuste podrá ser igual o menor que los cambios registrados en la Tasa de Cambio Oficial del Dólar Americano (US$) 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, **Superintendencia de Bancos de la Republica Dominicana** 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":**

Según descripciones técnicas de cada ítem (ver 2.8 Descripción de Bienes y Servicios)

Elegibilidad: Que el Proponente está legalmente autorizado para realizar sus actividades comerciales en el país.

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

3.5 Fase de Homologación

Una vez concluida la recepción de los **"Sobres A",** se procederá a la valoración de las muestras, si aplica, de acuerdo a las especificaciones requeridas en las Fichas Técnicas y a la ponderación de la documentación solicitada al efecto, bajo la modalidad **"CUMPLE/ NO CUMPLE".**

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 – Modificado y anexo en el portal de Compras y Contrataciones)**, 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 **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, en un plazo no mayor **(diez) 10 días**. 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 **Garantía Bancaria o Póliza de Fianza.** La vigencia de la garantía será de **(treinta) 30 a (noventa) 90 días, según plazo por cada item**, contados a partir de la constitución de la misma hasta el fiel cumplimiento del contrato.

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. Equipos tecnológicos (unidades) con características distintas a la del pliego.

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 podrá modificar, disminuir o aumentar hasta un podrá modificar, disminuir o aumentar hasta el cincuenta por ciento (50%), del monto del Contrato original del servicio, siempre y cuando se mantenga el de la contratación cuando se presenten circunstancias que fueron imprevisibles en el momento de iniciarse el proceso de contratación, y esa sea la única forma de satisfacer plenamente el interés público.

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 Vigencia del Contrato

La vigencia del Contrato será de **acuerdo a lo plasmado en cada item,** a partir de la fecha de la suscripción del mismo y hasta su fiel cumplimiento, de conformidad con el Cronograma de Entrega de Cantidades Adjudicadas, el cual formará parte integral y vinculante del mismo.

5.2.2 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.

Los Proveedores tendrán hasta el **plazo establecido en el punto 2.8 (Descripción de los Bienes y Servicios)**, en horario regular, para hacer la primera entrega de los Bienes que les fueren adjudicados; por lo que contarán con un período aproximado según el **plazo establecido en el punto 2.8 (Descripción de los Bienes y Servicios)** contados a partir de la Notificación de Adjudicación.

Item	Descripción	Cant.	Plazo
1	MIGRACIÓN DE PLATAFORMA FIREWALLS	1	8 Semanas
2	IMPLEMENTACION DE UNA HERRAMIENTA PARA ESCANEO DE VULNERABILIDADES	1	2 Semanas
3	DESKTOP CENTRAL ENTEPRISE EDITION DE LA HERRAMIENTA MANAGEENGINE PARA LA ASISTENCIA REMOTA A USUARIOS FINALES	1	3 Semanas
4	ROBUSTECIMIENTO DE LA PLATAFORMA CITRIX NETSCALER	1	8 Semanas
5	DISPOSITIVOS PARA LA REDUNDANCIA DE LA CONECTIVIDAD DE LAS REDES DE DATOS ENTRE LOS DIFERENTES NIVELES	1	8 Semanas
6	RACK PDU MONITOREABLES	1	8 Semanas
7	RENOVACION CENTRAL TELEFONICA (CISCO CUCM)	1	4 Semanas
8	RENOVACION SOPORTE PLATAFORMA HPE	1	3 Semanas

5.2.3 Modificación del Cronograma de Entrega

La Entidad Contratante, como órgano de ejecución del Contrato se reserva el derecho de modificar de manera unilateral 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.

5.2.4 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

Deberán coordinar previamente el momento de la entrega con la División de Compras y el Dpto. de Tecnología y deberá entregar con un personal calificado según requiera el producto.

Todos los bienes adjudicados deben ser entregados conforme a las especificaciones técnicas solicitadas, así como en el lugar de entrega convenido con **Superintendencia de Bancos de la Republica Dominicana,** 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 encuentran en la página de web: http://www.comprasdominicana.gov.do/**

- El **Formulario de Presentación de Oferta Económica (SNCC.F.033)** fue modificado y anexo, en el proceso, en el portal de Compras y Contrataciones. De no encontrarlo favor enviar correo para enviárselo.