**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-001/2019

Santo Domingo, Distrito Nacional
República Dominicana
**03 de Junio 2019**

**TABLA DE CONTENIDO**

## GENERALIDADES

### Prefacio

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

A continuación, se incluye una breve descripción de su contenido.

## PARTE 1 – PROCEDIMIENTOS DE LICITACIÓN

### Sección I. Instrucciones a los Oferentes (IAO)

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

### Sección II. Datos de la Licitación (DDL)

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

### Sección III. Apertura y Validación de Ofertas

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

### Sección IV. Adjudicación

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

## PARTE 2 - CONTRATO

### Sección V. Disposiciones sobre los Contrato

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

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

## PARTE 3 – ENTREGA Y 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-001/2019.**

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-001/2019
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 03 y Martes 04 de Junio 2019 |
| **2.** Período para realizar consultas por parte de los interesados | Miércoles 26 de Junio 2019 |
| **3.** Plazo para emitir respuesta por parte del Comité de Compras y Contrataciones | Viernes 5 de Julio 2019 |
| **4. Recepción de Propuestas y Apertura de: "Sobre A" y "Sobre B"** | **Miércoles 17 de Julio 2019 Desde las 10:00 am en el Salón de Conferencias de la SIB** |
| **5.** Verificación, Validación y Evaluación contenido de las Propuestas Técnicas "Sobre A" y Homologación de Muestras. | Del miércoles 17 al miércoles 24 de julio 2019 |
| **6.** Notificación de errores u omisiones de naturaleza subsanables. | Jueves 25 de Julio 2019 |
| **7.** Periodo de subsanación de ofertas | Del jueves 25 al lunes 29 de Julio 2019 |
| **8.** Período de Ponderación de Subsanaciones | Del lunes 29 al miércoles 31 de Julio 2019 |
| **9.** Evaluación Final de las Ofertas | Del miércoles 31 de Julio al miércoles 7 de Agosto 2019 |
| **10.** Adjudicación | Viernes 9 de Agosto 2019 |
| **11.** Notificación y Publicación de Adjudicación | Lunes 19 de Agosto 2019 |
| **12.** Plazo para la constitución de la Garantía Bancaria de Fiel Cumplimiento de Contrato | Lunes 26 de Agosto 2019 |
| **13.** Suscripción del Contrato | Lunes 16 de Septiembre 2019 |
| **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 | COMPUTADORA DE ESCRITORIO (DESKTOPS) | 90 | 1 MES | 4,896,000.00 |
| 2 | COMPUTADORA DE ESCRITORIO ESPECIALES (DESKTOP) | 10 | 1 MES | 604,000.00 |
| 3 | COMPUTADORA PORTÁTIL (LAPTOP) | 50 | 1 MES | 2,800,000.00 |
| 4 | ACTUALIZACIÓN PLATAFORMA DE FIREWALLS CHECKPOINT | 4 | 3 MESES | 9,758,953.00 |
| 5 | IMPLEMENTACIÓN SOLUCIÓN DE AUTENTICACIÓN DE DOBLE FACTOR CON TOKEN | 350 | 2 MESES | 4,000,000.00 |
| 6 | IMPLEMENTACIÓN DE UN (INSTRUSION DETECTION PREVENTION SYSTEMS) (IDPS) | 2 | 3 MESES | 4,437,000.00 |
| 7 | IMPLEMENTACIÓN DE UN EQUIPO WEB APPLICATION FIREWALL | 1 | 3 MESES | 5,082,000.00 |
| 8 | IMPLEMENTACIÓN DE HERRAMIENTA DE CLASIFICACIÓN DE LA INFORMACIÓN | 1 | 3 MESES | 6,700,000.00 |
| 9 | IMPLEMENTACIÓN DE UNA HERRAMIENTA DE CUENTAS PRIVILEGIADAS | 1 | 3 MESES | 3,200,000.00 |
| 10 | IMPLEMENTACIÓN DE UNA HERRAMIENTA DE SEGURIDAD DATA BASE FIREWALL | 1 | 3 MESES | 8,840,000.00 |
| 11 | HERRAMIENTA PARA ESCANEO DE VULNERABILIDADES POR 3 AÑOS | 1 | 3 MESES | 500,000.00 |
| 12 | GESTIÓN Y CORRELACIÓN DE EVENTOS DE INFORMACIÓN DE SEGURIDAD (SIEM) | 1 | 3 MESES | 4,080,000.00 |
| 13 | ROBUSTECIMIENTO DE PLATAFORMA BLADE | 1 | 2 MESES | 40,000,000.00 |
| 14 | SERVICIO DE COLOCACIÓN PARA DATACENTER (COLLOCATION) POR 3 AÑOS | 1 | 2 MESES | 18,000,000.00 |

## 1. COMPUTADORA DE ESCRITORIO (DESKTOPS)

| | |
|---|---|
| **Descripción** | Computadora de escritorio (DESKTOP) |
| **Cantidad** | 90 |
| **Procesador** | Intel Core i7 – 8va. Generación o Superior |
| **Memoria Ram** | 8GB DDR4 1600Mhz o superior |
| **Form Factor** | SFF |
| **Disco** | 1 TB SATA o superior |
| **Multimedia** | Unidad lectora DVD / CD, Bocinas internas |
| **Video** | 1 GB tarjeta de video o superior, con HDMI Port |
| **Red** | RJ45 10/100/1000 |
| **Sistema operativo (SO)** | Windows 10 x64 Professional en español de fábrica. |
| **Monitor** | 21 Pulgadas LED Widescreen con HDMI Port de la misma marca que el Desktop y cable HDMI incluido. |
| **Teclado** | Teclado estándar en español **USB** |
| **Mouse** | Mouse **USB** Óptico |
| **Garantía** | 3 años de Garantía en Piezas y servicio **Full en sitio** |
| **Marca** | Equipo de Marca, 100% Original, no se aceptan equipos de reemplazo, refurbished, remanufacturados, o reempacados, debe ser 100% nuevo. |
| **Tiempo de entrega** | 1 Mes |

## 2. COMPUTADORA DE ESCRITORIO ESPECIALES (DESKTOPS)

| | |
|---|---|
| **Descripción** | COMPUTADORA DE ESCRITORIO ESPECIALES (DESKTOP) |
| **Cantidad** | 10 |
| **Procesadorb** | Intel Core i7 – 8va. Generación o Superior |
| **Memoria Ram** | 16GB DDR4 1600Mhz o superior |
| **Form Factor** | TOWER |
| **Disco** | 1 TB SATA o superior |
| **Multimedia** | Unidad lectora DVD / CD, Bocinas internas |
| **Video** | 1 GB tarjeta de video o superior, con HDMI Port |
| **Red** | RJ45 10/100/1000 |
| **Sistema operativo (SO)** | Windows 10 x64 Professional en español de fábrica. |

| | |
|---|---|
| **Monitor** | 24 Pulgadas LED Widescreen con HDMI Port de la misma marca que el Desktop y cable HDMI incluido. |
| **Teclado** | Teclado estándar en español **USB** |
| **Mouse** | Mouse **USB** Óptico |
| **Garantía** | 3 años de Garantía en Piezas y servicio **Full en sitio** |
| **Marca** | Equipo de Marca, 100% Original, no se aceptan equipos de reemplazo, refurbished, remanufacturados, o reempacados, debe ser 100% nuevo. |
| **Tiempo de Entrega** | 1 Mes |

## 3. COMPUTADORA PORTÁTIL (LAPTOP)

| | |
|---|---|
| **Descripción** | Computadora portátil (LAPTOP) |
| **Cantidad** | 50 |
| **Procesador** | Intel Core i7 – 8va. Generación. |
| **Memoria Ram** | 8GB DDR4 1600Mhz o superior |
| **Disco** | 1 TB SATA o superior |
| **Multimedia** | Unidad DVD +/-RW. Bocinas, micrófono, cámara frontal. |
| **Tarjeta Video** | Intel HD Graphic o superior |
| **Red** | RJ45 10/100/1000 |
| **WiFi** | B/G/N/AC con bluetooth |
| **Puertos** | Debe incluir USB3, HDMI |
| **Ranura Expansión** | SD, SDHC |
| **Sistema Operativo** | Windows 10 x64 Profesional en español de fábrica. |
| **Pantalla** | 15.6 Pulgadas LED HD |
| **Form Factor** | Business (Ejecutivo). Chasis aluminio reforzado. |
| **Teclado** | Teclado en español. Metal resistente a derrames. |
| **Batería** | Seis celdas o superior. |
| **Garantía** | 3 años (en piezas y servicios **en sitio Full**, incluyendo batería y cargador) |
| **Cargador** | Original, nuevo, de la misma marca que la Laptop, no se aceptan cargadores de reemplazo, ni refurbished. |
| **Marca** | Equipo de Marca, 100% Original, no se aceptan equipos de reemplazo, refurbished, remanufacturados, o reempacados, debe ser 100% nuevo. |
| **Bulto** | Bulto Ejecutivo para laptop. Requiere Muestra |

| | |
|---|---|
| **Tiempo de Entrega** | 1 Mes |
| **Muestra** | Se requiere muestra del bulto. |

## 4. ACTUALIZACIÓN PLATAFORMA DE FIREWALLS CHECKPOINT

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Sustitución del Checkpoint modelo 4400 por el Checkpoint modelo 5800 | UN | 4 |
| B | 3 Años de Garantía | UN | 1 |

### 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 migración 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

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

- Stateful Inspection Firewall
- Application Control and URL filtering
- User Identity Acquisition
- Anti-Bot and Anti-Virus
- Sandboxing
- IPSec VPN
- Security Policy Management
- Logging y Status
- Event Logs & Report

**Stateful Inspection Firewall**

- 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.

- 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.

**Filtrado URL y Control de Aplicación**

- La base de datos de control de aplicaciones debe contener más de 6000 aplicaciones conocidas.
- La solución debe proveer control granular de seguridad de al menos 250,000 widgets Web 2.0
- La solución debe tener una categorización de URL que exceda los 200 millones de URL.
- La solución debe ser capaz de crear una regla de filtro con múltiples categorías.
- La solución debe ser capaz de crear un filtrado para un sitio soportado por múltiples categorías.
- La solución debe tener granularidad de usuarios y grupos con reglas de seguridad.
- La solución debe tener una interfaz fácil de usar, que permita buscar aplicaciones y URLs.
- La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
- La política de seguridad de control de aplicación y filtrado URL debe ser capaz de ser definida por identidades de usuarios.
- La base de datos de filtrado URL y control de aplicación debe ser actualizada por un servicio basado en la nube.
- La solución debe tener reglas de seguridad unificadas para el control de aplicación y filtrado URL.
- La solución debe proporcionar un mecanismo para informar o preguntar a usuarios en tiempo real para educarlos o confirmar acciones basadas en la política de seguridad.
- La solución debe proporcionar un mecanismo para limitar el uso de aplicaciones basado en el consumo de ancho de banda.
- La solución debe permitir excepciones de red basadas en objetos de red definidos.
- La solución debe proporcionar la opción para modificar la Notificación de bloqueo y redirigir al usuario a una página de remediación.
- La solución debe incluir mecanismos de Black y White Lists para permitir al administrador denegar o permitir URLs específicas, sin importar su categoría.

- La solución debe tener mecanismos de bypass configurables.
- La solución debe proporcionar un mecanismo de override en la categorización para la base de datos de URL.
- La política de seguridad de filtrado URL y control de aplicación debe reportar un conteo de utilización de las reglas.

**Adquisición de Identidad del usuario**

- Debe ser capaz de adquirir la identidad del usuario buscando en eventos de seguridad basados en Microsoft Active Directory.

- Debe tener un método de autenticación de Identidad del Usuario a través del browser para activos o usuarios fuera del dominio.

- Debe soportar ambientes de terminal server.

- La solución debe integrarse perfectamente con los servicios de directorio, IF-MAP y Radius.

- El impacto en los controladores de dominio debe ser menor a 3%.

- La solución de identidad debe soportar terminal server y servidores citrix.

- La solución debe permitir la identificación a través de un proxy.

- Debe ser capaz de adquirir la identidad del usuario desde Microsoft Active Directory sin la instalación de ningún tipo de agente en los controladores de dominio.

- Debe soportar el uso de grupos de LDAP anidados.

- Debe ser capaz de compartir y propagar las identidades de los usuarios entre múltiples Security Gateways.

**Anti-Bot y 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.

**Sandboxing**

- La solución debe proporcionar la capacidad de protegerse contra ataques de malware desconocido y de día cero antes de que se creen protecciones de firmas estáticas.

Topologías de despliegue:

- La solución debe ser parte de una arquitectura completa de prevención de amenazas de múltiples capas.
- La solución debe ser compatible con la emulación de amenazas basada en la red.
- La solución debe ser compatible con la emulación de amenazas basada en host.
- La solución debe proporcionar implementaciones tanto en el sitio como en la nube.
- La solución debe ofrecer una opción de implementación que no requiera ninguna infraestructura adicional.
- La solución debe admitir la implementación en modo en línea.

- La solución debe admitir la implementación en modo MTA (Mail Transfer Agent).

- La solución debe admitir la implementación en modo puerto TAP / SPAN.

- El dispositivo debe soportar la instalación de clústeres

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, Zip

Soporte Sistema Operativo:

- El motor de emulación debe ser compatible con múltiples sistemas operativos, como Windows 7 y Windows 10, incluidas las imágenes customizadas.

- El motor debe detectar llamadas a la API, cambios en el sistema de archivos, registro del sistema, conexiones de red, procesos del sistema.

- La solución debe ser compatible con el análisis estático para Windows, Mac OS, Linux o cualquier plataforma x86.

Tecnología Sandboxing

- El motor de emulación debe poder inspeccionar, emular, prevenir y compartir los resultados del evento de sandbox en la infraestructura antimalware.

- La solución permitiría la emulación de tamaños de archivo mayores a 10 MB.

- Detección y prevención inmediata: la solución debe detectar el ataque en la etapa de explotación, es decir, antes de que se ejecute el código de Shell y antes de que se descargue / ejecute el malware.

- La solución debería poder detectar ROP y otras técnicas de explotación (por ejemplo, escalada de privilegios) mediante la supervisión del flujo de la CPU.

- La solución debe ser capaz de escanear enlaces dentro de correos electrónicos para detectar y prevenir malware de día cero y desconocido.

- El tiempo promedio de emulación de un presunto veredicto de malware como benigno no debe ser más de 1 minuto.

- El tiempo promedio de emulación de un presunto veredicto de malware como malware no debe ser superior a 3 minutos.

- La solución de emulación de amenazas debe permitir la "Restricción geográfica", que permite que las emulaciones se limiten a un país específico.

- La solución debe proporcionar la capacidad de aumentar la seguridad al compartir automáticamente la información de nuevos ataques con otros gateways mediante actualizaciones de firmas, etc.

- Detección de actividad del sistema

La solución debe monitorear la actividad sospechosa en:

- Llamadas API

- Cambios en el sistema de archivos

- Registro del sistema

- Conexiones de red

- Procesos del sistema

- Creación y eliminación de archivos

- Modificación de archivos

- Inyección de código de kernel

- Modificaciones al kernel (cambios en la memoria realizados por el código del kernel, no por el hecho de que se haya cargado un controlador)

- Comportamiento del código del kernel (monitorear la actividad del código de modo no usuario)

- Interacción directa del CPU

Tecnología Anti-Evasión

- La solución debe tener capacidades anti evasión que detecten la ejecución de sandbox.

- El motor de emulación debe tener capacidades de detección anti-vm.

- La solución debe ser resistente a los retrasos implementados en el código de shell o en las etapas de malware.

- La solución debe ser resistente a los casos en los que el código de shell o el malware se ejecuten solo al reiniciar o apagar el equipo.

- La solución debe ser resistente a los casos en que el código de shell o el malware no se ejecutaría si detectan la existencia de un entorno virtual.

- La solución debe emular actividades reales del usuario, como clics del mouse, pulsaciones de teclas, etc.

- La solución debe emular actividades reales del usuario, como clics del mouse, pulsaciones de teclas, etc.

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

Extracción de amenazas (depuración / aplanamiento de archivos)

- La solución debe eliminar las amenazas y eliminar el contenido explotable, incluido el contenido activo y los objetos incrustados.
- La solución debe poder reconstruir archivos con elementos seguros conocidos.
- La solución debe proporcionar la capacidad de convertir archivos reconstruidos a formato PDF.
- La solución debe mantener la flexibilidad con las opciones para mantener el formato de archivo original y especificar el tipo de contenido que se eliminará.

**VPN IPSec**

- 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.
- La solución debe soportar la integridad de los datos con MD5, SHA1 SHA-256, SHA-384 y AES-XCBC.
- La solución debe incluir soporte para VPN site-to-site en las siguientes topologías:
  - Malla completa (full mesh)
  - Estrella (star)

- Hub and Spoke

- La solución debe soportar la configuración VPN con una GUI que permita añadir objetos mediante drag and drop a las comunidades VPN.

- La solución debe soportar VPNs SSL sin clientes para acceso remoto.

- La solución debe soportar VPNs L2TP.

- La solución debe permitir al administrador aplicar reglas de seguridad para controlar el tráfico dentro de la VPN.

- La solución debe soportar VPNs basadas en el dominio y basadas en rutas utilizando VTIs y protocolos de enrutamiento dinámico.

- La solución debe incluir la capacidad para establecer VPNs con gateways con IPs públicas dinámicas.

- La solución debe incluir compresión IP para VPNs client-to-site y site-to-site.

**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.

**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.

**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 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 Anti-Virus, Anti-Bot, 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.

**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.

  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
  - Servicios principales que crearon mayor carga para el tráfico cifrado.
  - Usuarios principales de VPN que realizan las conexiones de más larga duración

**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.

- Se requiere dos licencias de Management Center para los Firewalls, appliance virtual para infraestructura VMWare 6.5 o superior.

## 4. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Estas aplicaciones deben ser suplidas y manejadas exclusivamente por el proveedor.

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

- El proveedor debe poseer la certificaciones necesarias para implementar la solución.

- El proveedor debe proporcionar entrenamiento de la solución.

- El proveedor debe migrar e implementar la plataforma de Firewall con las políticas definidas de la institución una vez sea revisado y aprobado por el personal de la SIB.

## 5. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- Debe implementar los nuevos firewalls y realizar la migración de la plataforma actual
- 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

## 6. PERFIL PROFESIONAL:

- El proveedor del software del Gateway 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 firewalls para empresa, firewalls basada en datos independientes de la seguridad de la industria.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta de Next Generation Firewalls.

- El proveedor debe ser capaz de atender todo el alcance de los requisitos de Gateway de seguridad, incluido el rendimiento, velocidad de conexión y habilitación de la aplicación de seguridad de próxima generación para todas las implementaciones de red, desde la pequeña oficina hasta el centro de datos en un único dispositivo de hardware.

## 5. IMPLEMENTACIÓN SOLUCIÓN DE AUTENTICACIÓN DE DOBLE FACTOR CON 350 TOKENS

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Solución Autenticación Doble Factor | UN | 350 |
| B | 3 Años de Mantenimiento, Soporte y Garantía | UN | 1 |

## 1. PLANTEAMIENTO DE LA NECESIDAD

Debido a que la gran mayoría de los servicios y sistemas que utilizamos en el día a día requieren como único control de acceso un nombre de usuario y contraseña. En estos casos, la clave actúa como una llave digital que le permite a un usuario identificarse en el sistema para poder acceder a información sensible. De este modo, dicha contraseña protege los datos privados del acceso no autorizado por parte de terceros. En tal sentido, se requiere implementar una solución que permita la autenticación de doble factor con token y con esto agregar una capa de seguridad adicional al proceso de inicio de sesión con el fin de mitigar cualquier crimen digital y el fraude en internet.

## 2. OBJETIVOS

### 2.1. Objetivo General

Implementar una solución de autenticación de doble factor con token para la Superintendencia de Bancos.

### 2.2. Objetivos Específicos

- Minimizar significativamente el riesgo de fraudes y otro delito electrónico
- Garantizar autenticación segura

## 3. FUNCIONALIDADES DE SOLUCIÓN AUTENTICACIÓN CON TOKEN

**Auth manager**

- Este dispositivo deberá generar una contraseña única (OTP one time password por sus siglas en ingles).
- Se requiere que el algoritmo utilizado en la solución de autenticación sea basado en sincronía por tiempo.
- La solución de autenticación deberá estar disponible en su versión de Appliance virtual HA, para infraestructura VMWare 6.5 o superior.
- La solución de autenticación deberá integrarse con la base de datos de usuarios existente, esta base de datos de usuarios se encuentra actualmente en un dominio activo y se puede acceder utilizando LDAP.
- Se requiere que tenga integración nativa con un directorio activo de Microsoft.
- Deberán existir diferentes agentes para integrar nuestras aplicaciones, es decir debe ser fácil y flexible en su integración.
- La solución de autenticación debe contar con una consola remota para llevar a cabo la administración de la solución, de preferencia la consola deberá ser tipo web, y las tareas mínimas que se deben poder realizar en la consola son:
    - Creación de un usuario
    - Asignación de dispositivos
    - Poder habilitar/deshabilitar un dispositivo

- La solución de autenticación debe contar con una bitácora de las actividades que se realizan dentro de la misma; como mínimo se deben registrar:
    - Actividades administrativas
    - Autenticación de usuarios.

- La solución de autenticación deberá contar con una opción que nos permita habilitar hasta un 10% más de dispositivos de autenticación (tokens); los cuales deberán estar disponibles por demanda (on demand tokens). Con la finalidad de garantizar el acceso y asegurar así la continuidad de negocio.

- Para el caso de las funciones administrativas, el registro de la bitácora deberá tener al menos
    - Hora y Fecha del momento en el que se llevó a cabo el movimiento
    - Debe registrar cuando un usuario es creado o borrado
    - Debe registrar cuando se asigna o desasigna un dispositivo, así como la información para identificar el dispositivo.

- Para el caso de la autenticación del usuario, el registro de la bitácora deberá tener al menos
    - Hora de acceso
    - Fecha de acceso
    - Identificación del dispositivo asignado
    - Nombre del usuario

- La solución de autenticación debe permitir la consulta de la bitácora en tiempo real.
- La solución de autenticación deberá contar con un módulo para generación de reportes en el cual se puedan extraer registros de la bitácora.

- La solución de autenticación debe permitir la creación de grupos de usuarios.
- La solución debe contar con los mecanismos para respaldar la información de usuarios y los dispositivos. Con la finalidad de poder restaurar un equipo en caso de desastre.
- La solución de autenticación debe contar con una configuración de alta disponibilidad, si un servidor de autenticación no responde o no está disponible el segundo en la configuración deberá llevar a cabo la autenticación del usuario.
- La solución de autenticación debe permitir el balanceo de carga, si uno de los servidores de autenticación no responde o no está disponible contar con una configuración de alta disponibilidad.

**Token**

- Se deberá comprobar que con el uso de un dispositivo se puedan tener 2 factores de autenticación; el primero por algo que el usuario sabe (contraseña) y el segundo por algo que el usuario tiene (Token contraseña dinámica).
- Este dispositivo deberá generar una contraseña única (OTP one time password por sus siglas en ingles), por minuto.
- La solución de autenticación debe permitir el uso de una clave personal (NIP) en conjunto con la clave generada por el dispositivo para llevar a cabo la autenticación. (doble factor)
- Se busca que el dispositivo que genera la clave única, no requiera mantenimiento.
- Para el caso de los dispositivos de autenticación de hardware, deberá tener un tiempo de vida de 5 años, en caso de falla el proveedor deberá reemplazar y entregar el dispositivo al usuario final sin un costo adicional para la solicitante.

- Se busca que el dispositivo físico que genera la clave única, no debe requerir algún tipo de programación o inicialización para su uso, en caso de requerirlo el proveedor entregara el dispositivo al solicitante listo para su uso.
- Deberán tener en existencia diferentes tipos de autenticadores (tokens), aunque la primera opción preferida será el dispositivo físico:
    - Software (ej Windows)
    - Pueda ser instalado en teléfonos ios y Android

## 4. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- El proveedor debe poseer las certificaciones de la industria de la solución.

- El proveedor debe proporcionar entrenamiento 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 de implementar la solución de autenticación de doble factor en la institución y validar su funcionamiento e integración con las aplicaciones definidas, una vez sea revisado y aprobado por el personal de la SIB.

## 5. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- Propuesta de solución autenticación de doble factor
- Plan de trabajo de Implementación de solución autenticación de doble factor.
- Solución autenticación de doble factor de la Superintendencia de Bancos en funcionamiento e integrada con las aplicaciones definidas.

## 6. PERFIL PROFESIONAL

- El proveedor de la solución de doble factor 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 solución autenticación de doble factor con token.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta de Autenticación de doble factor.

- 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 autenticación de doble factor con token.

## 6. IMPLEMENTACIÓN DE UN INTRUSION DETECTION PREVENTION SYSTEMS (IDPS)

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Sistema Detección y Prevención de Intrusiones | UN | 2 |
| B | 3 Años de Mantenimiento, Soporte y Garantía | UN | 1 |

### 1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente la SIB tiene implementado una plataforma de software IPS (Intrusión Prevention System) integrado en el firewall perimetral para la detección y protección del perímetro de su red. Sin embargo, a medidas que los ataques cibernéticos evolucionan, la seguridad de la red requiere una visibilidad e inteligencia sin precedentes que cubran todas las amenazas para una protección integral con las diferentes agendas y responsabilidades de la organización, en tal sentido se necesita un mecanismo de Instrucción Detection Prevention System (IDPS) que no esté integrado en otra solución para lograr proporcionar un nivel más profundo de seguridad y visibilidad para la institución.

### 2. OBJETIVOS

#### 2.1. Objetivo General

Implementar un Intrusion Detection and Prevention System (IDPS) en el perímetro de la red de la Superintendencia de Bancos.

#### 2.2. Objetivos Específicos

- Vigilar el tráfico de una red
- Lanzar una alerta en caso de actividades maliciosas o comportamiento anómalo
- Registrar la intrusión identificada
- Prevenir explotaciones de vulnerabilidad
- Bloquear códigos extraños
- Bloquear ataques de día cero

## 3. FUNCIONALIDADES DE PLATAFORMA DE IDPS

El Intrusion Detection Prevention System (IDPS) debe ser capaz de soportar las siguientes capacidades de seguridad de próxima generación.

- Protection Against Advanced Threats
- Real-time Contextual Awareness
- Intelligent Security Automation
- Application Control
- Security Intelligence
- Retrospective Remediation
- Correlación de Eventos & Reportes
- Portal de administración

**Protection Against Advanced Threats**

- Realizar un seguimiento continuo de los archivos hasta comprobar si son desconocido o seguro.

- Actualizar automáticamente las listas negras para bloquear la comunicación a sitios maliciosos, incluidos no solo los servidores de comando y control de malware, sino también el correo no deseado, el phishing, la red de bots y los servidores proxy abiertos y las fuentes de retransmisión.

**Real-time Contextual Awareness**

- Incluir información de los datos recopilados y analizados sobre aplicaciones, usuarios, dispositivos, sistemas operativos, vulnerabilidades, dispositivos móviles, aplicaciones del lado del cliente, servicios, procesos, comportamientos de red, archivos y amenazas.

- Usar en sus reglas de Intrusion Prevention System (IPS) los datos contextuales para proporcionar un nivel granular extraordinariamente de alta protección.

**Intelligent Security Automation**

- Identificar las amenazas que importan más al correlacionar automáticamente los eventos de intrusión con las vulnerabilidades encontradas.

- Implementar una mejor seguridad al analizar las redes, debilidades y generando las políticas de protección adecuadas.

- Acelerar el análisis forense vinculando a los eventos de usuarios.

- Evitar las amenazas rápidamente con un flujo de trabajo de remediación automatizada.

**Security Intelligence**

- Tener capacidad de realizar un seguimiento a los atacantes conocidos, direcciones IP falsas debido a que las fuentes de información de inteligencia se actualizan regularmente.

- Garantizar que el sistema utilice información actualizada para filtrar el tráfico de red, direcciones IP maliciosas, nombres de dominio y las URL que representan amenazas de seguridad como malware, spam, botnets y phishing.

- Permitir agregar a la lista negra manualmente direcciones IP, URL o nombres de dominio específicos de muchas maneras, según sus necesidades.

- Eliminar falsos positivos mediante listas blanca

- Aplicar listas negras por zona de seguridad

**Correlación de Eventos & Reportes**

- Debe de proporcionar un sistema de informes flexible que le permite generar rápida y fácilmente informes de varias secciones con las vistas de eventos o paneles. También poder diseñar sus propios informes personalizados desde cero.

- Especificar las búsquedas de datos y los formatos para el informe y sus secciones.

- Crear tantas plantillas de informes según se necesite en la institución

- La solución debe de obtener información precisa sobre los posibles incidentes de seguridad y amenazas hacia nuestros sistemas. La respuesta en forma de alarmas, puede desencadenar un plan de acción proactiva e inteligente evitando el daño a la organización en tiempo real.

- Emitir avisos de forma inmediata a través de alarmas, comunicando las causas de la incidencia, con la finalidad de establecer una resolución adecuada de la situación.

- Analizar eventos y su consiguiente correlación con el fin de reducir el número de falsos positivos e identificar en la mayor brevedad los cambios de estado y alteraciones de los comportamientos anómalos en el Intrusion Detection Prevention System (IDPS).

**Portal de Administración**

- Incluir un acceso a través de browser para observar en modo sólo lectura y escritura las políticas de seguridad, gestionar los logs generados por los usuarios.

- Proporcionar accesos de lectura a los ejecutivos a sin la necesidad de tener que utilizar el acceso de administración.

- El Intrusion Detection Prevention System (IDPS) debe soportar excepciones de red, tomando en cuenta la fuente, el destino, el servicio o una combinación de los tres.

- El appliance de Intrusion Detection Prevention System (IDPS) debe tener una correlación de eventos centralizada y mecanismo de reporte.

- El administrador debe ser capaz de activar automáticamente nuevas protecciones, basadas en parámetros configurables (impacto en el rendimiento, severidad de la amenaza, nivel de confianza, protecciones de cliente, protecciones de servidor)

- El Intrusion Detection Prevention System (IDPS) debe poder detectar y prevenir las siguientes amenazas: Mal uso de protocolos, comunicaciones de malware, intentos de tunneling y tipos de ataques genéricos sin firmas predefinidas.

- Para cada protección la solución debe incluir el tipo de protección (relacionado al servidor o al cliente), severidad de la amenaza, impacto en rendimiento, nivel de confianza y referencia de la industria.

- El Intrusion Detection Prevention System (IDPS) debe ser capaz de recopilar la captura de paquetes para protecciones específicas.

- El Intrusion Detection Prevention System (IDPS) debe detectar y bloquear ataques de capas de aplicación y de red, protegiendo al menos los siguientes servicios: email services, DNS, FTP, Windows services, SNMP.

- El Intrusion Detection Prevention System (IDPS) debe incluir la capacidad de detectar y bloquear tráfico peer-to-peer utilizando técnicas de evasión.

- El administrador debe ser capaz de definir exclusiones de hosts y de red de la inspección de Intrusion Detection Prevention System (IDPS).

- La solución debe proteger de DNS Cache Poisoning, y prevenir a usuarios de acceder a direcciones de dominios bloqueados.

- La solución debe proporcionar protecciones a protocolos de VoIP.

- El Intrusion Detection Prevention System (IDPS) debe detectar y bloquear aplicaciones de control remoto, incluyendo aquéllas que son capaces de realizar tunneling sobre tráfico HTTP.

- La Solución debe cumplir con la aplicación de protocolo Citrix.

- La solución debe permitir al administrador bloquear tráfico entrante y saliente basado en países, sin la necesidad de gestionar manualmente los rangos de IP correspondientes al país.

- El Intrusion Detection Prevention System (IDPS) debe tener opciones para crear perfiles para protecciones basadas en cliente o servidor, o una combinación de ambas.

- El Intrusion Detection Prevention System (IDPS) debe proveer al menos dos políticas/perfiles predefinidos que puedan ser utilizados inmediatamente.

- El Intrusion Detection Prevention System (IDPS) debe tener un mecanismo de fail-open, configurable basado en los límites de uso de memoria y CPU de los Appliance.

- El Intrusion Detection and Prevention System (IDPS) debe proporcionar un mecanismo automático para activar o gestionar nuevas firmas desde las actualizaciones.

- El Intrusion Detection Prevention System (IDPS) debe tener 8 puertos de 1G.

- Discos duros de estado sólido

- Debe ser escalable

- Conjunto diverso de opciones de conectividad de medios.

- Alto tiempo medio entre fallos (MTBF).

- Fuentes de alimentación redundantes para resistencia a fallos.
- Puerto de administración dedicado, fuera de banda.
- NGIPS adaptativos en tiempo real (basados en la evaluación dinámica de la red: automáticamente "sabe" lo que hay en la red).
- Capacidad para automatizar completamente tareas como informes, actualizaciones, copias de seguridad, etc.
- Priorización automática de eventos de amenazas según la relevancia para el entorno protegido.
- Capacidad para ajustar automáticamente la política de intrusión basada en dispositivos en un entorno protegido.
- Lista blanca de diversos conjuntos de dispositivos (impresoras, enrutadores, etc.) / Sistemas operativos / aplicaciones / servicios.
- Capacidad de utilizar datos de flujo generados externamente.
- Habilidad para buscar patrones de tráfico anómalos.
- Capacidad para identificar a los usuarios de forma activa y pasiva a través de múltiples fuentes (AD, Oracle, POP / IMAP, etc.).
- Reglas de correlación personalizables para la detección y remediación únicas específicas del cliente.
- Agregación de múltiples eventos en indicaciones de compromiso vinculados a un host específico.
- API de entrada para actualizar la información contextual específica del host.
- Soporte totalmente integrado para el etiquetado de grupos de seguridad para permitir una seguridad basada en políticas independiente de la topología.
- Notificación retrospectiva sobre contenido de archivos maliciosos.
- Visibilidad y control de diversos tipos de archivos en la capa de red.
- Detección de malware en tiempo real y en la nube.

- Lista negra personalizada de tipos de archivos o archivos individuales.
- Trayectoria detallada de la red para el control de brotes y la remediación.
- Integración con sistemas de protección de puntos finales.
- Bloqueo integrado de URL maliciosas según el tipo (C&C, spam, etc.).
- Captura de archivos para archivos maliciosos, buenos y / o desconocidos.
- Habilidad para ser monitoreado por MSP.
- Capacidad de ser gestionado por MSP.
- API para la salida del evento a SIEM.
- API para la entrada de datos de conciencia ambiental (exploración de vulnerabilidad, perfiles de host).
- API para proporcionar instrucciones a productos de terceros para la reparación automática.
- Monitoreo completo de SNMP (Trampa, MIB).
- Soporte para protocolos estándar de la industria como NetFlow y WCCP.
- La solución debe ser compatible con Perfect Forward Secrecy (PFS, suites de cifrado ECDHE).
- La solución debe ser compatible con AES-NI, AES-GCM para mejorar el rendimiento.
- La emulación de amenazas / sandboxing debe integrarse con la Inspección SSL.
- La solución puede aprovechar la base de datos de filtrado de URL para permitir que el administrador cree una política de inspección granular de https.
- El descifrado SSL puede basarse en una amplia variedad de criterios, incluidos la red, el usuario, la aplicación, el conjunto de cifrado, la versión TLS, el estado del certificado y la categoría de URL.
- La solución puede inspeccionar el filtrado de URL basado en HTTPS sin requerir descifrado SSL.

- Se requiere dos licencias de Management Center para los IDPS, appliance virtual para infraestructura VMWare 6.5 o superior.

## 4. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Las aplicaciones deben ser suplidas y manejadas exclusivamente por el proveedor.
- El proveedor debe poseer la certificaciones necesarias para implementar la solución.
- El proveedor debe proporcionar entrenamiento de la solución.
- El proveedor debe proporcionar entrenamiento de la solución a personal de la SIB.
- 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 plataforma de Intrusion Detection Prevention System (IDPS) de la institución una vez sea revisado y aprobado por el personal de la Superintendencia de Bancos (SIB).

## 5. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- Propuesta de plataforma de IDPS
- Plan de trabajo de Implementación de plataforma de IDPS
- Plataforma de IDPS de la Superintendencia de Bancos debe quedar en funcionamiento con los perfiles de protección definidos para la infraestructura de la SIB.

## 6. PERFIL PROFESIONAL

- El proveedor del Appliance IDPS 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 IDPS para empresa, independientes de la seguridad de la industria.

- El proveedor debe ser capaz de atender todo el alcance de los requisitos de appliance de seguridad, incluido el rendimiento, velocidad de conexión desde la pequeña oficina hasta el centro de datos en un único dispositivo de hardware.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta Intrusion Detection Prevention System (IDPS).

- 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 Intrusion Detection Prevention System (IDPS)

## 7. IMPLEMENTACION DE UN EQUIPO WEB APLICATION FIREWALL

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Web Application Firewall | UN | 1 |
| B | 3 Años de Soporte, Mantenimiento Premium | UN | 1 |

### 1. PLANTEAMIENTO DE LA NECESIDAD

Debido a que en el desarrollo de una aplicación web suelen detectarse vulnerabilidades y en algunas circunstancias no es posible mitigarlas de forma inmediata, en la Superintendencia de Bancos (SIB) actualmente es necesario un mecanismo que nos ofrezca protección a ataques maliciosos como (inyección de SQL y los ataques de scripts) que pueden explotar vulnerabilidades en aplicaciones web ya existentes en la institución. Por eso existe la necesidad de un adquirir un equipo Web Application Firewall (WAF) para proteger a los servidores de aplicaciones web de determinados ataques específicos en Internet.

### 2. OBJETIVOS

#### 2.1. Objetivo General

Implementar un Web Application firewall en la red de la Superintendencia de Bancos.

#### 2.2. Objetivos Específicos

- Proteger de ataques de inyección SQL
- Proteger de scripts entre sitios
- Proteger de ataques común aplicaciones web, como la inyección de comandos, el contrabando de solicitudes HTTP, la división de respuestas HTTP y el ataque de inclusión remota de archivos

- Detectar errores de configuración de aplicaciones comunes (por ejemplo, Apache, IIS, etc.).
- Prevenir contra bots, rastreadores y escáneres.

## 3. FUNCIONALIDADES DE PLATAFORMA DE WEB APPLICATION FIREWALL (WAF)

- El modelo positivo de seguridad deberá definir lo que está permitido y bloquear todo lo demás. Deberá incluir direcciones URL, directorios, cookies, campos, parámetros (identificando además el formato y tipo de estos), métodos HTTP.
- Para facilitar la configuración del modelo positivo de seguridad, el dispositivo deberá aprender automáticamente la estructura y los elementos de la aplicación de manera constante y sin intervención humana.
- La solución deberá contar con un modo aprendizaje para rastrear cambios continuos en las aplicaciones web, deberá reconocer cambios en la aplicación y simultáneamente protegerlas.

**Deberá contar con las siguientes características:**

- Deberá aprender los valores aceptables para los campos de ingreso de datos con base en el registro de la actividad.
- Los valores aprendidos podrán ser utilizados como la configuración inicial sobre la que se revisarán los datos ingresados en el modelo positivo de seguridad.
- El modo aprendizaje, deberá aprender la estructura y elementos de la aplicación (directorios, url´s, parámetros, cookies) y el comportamiento esperado del usuario (longitud del valor esperado, caracteres aceptados, si el parámetro es de sólo lectura o editable por el usuario) y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad.
- La configuración aprendida deberá ser accesible y modificable para el administrador del dispositivo.
- La solución deberá correlacionar múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.
- La solución deberá permitir la modificación de reglas de seguridad. Los administradores deberán poder definir reglas para el modelo de seguridad positivo o negativo y deberán crear reglas de correlación con múltiples criterios.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación Web. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
- Estado de autenticación de la sesión web
- Por el URL de autenticación y el resultado del intento de autenticación

- Por URL, a través del prefijo, ruta o host.
- Por la existencia o contenido de cualquier Header HTTP
- Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares), ya sea en el HTTP Request o el Response por parte del servidor Web
- Tipo de archivo siendo transmitido en cualquier sentido
- Host o dominio accedido
- Métodos HTTP usados
- Número de ocurrencias en intervalos de tiempo definidos
- La existencia o contenido de cualquier Parámetro web
- Por el protocolo usado, HTTP o HTTPS
- IPs de origen y destino
- Por la existencia o contenido de Cookies o el identificador de Sesión
- Response Code y Headers en el Response HTTP por parte del servidor Web
- Hora del Dia
- Por usuario firmado en el aplicativo web
- User-Agent
- Referer-URL
- Tiempo de respuesta o tamaño de la respuesta HTTP
- La solución deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente.
- La solución deberá cumplir con todos los criterios de evaluación del WAFEC definidos por el Web Application Security Consortium.
- La solución deberá proporcionar el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación web.
- La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
- La solución deberá tener la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.
- La solución deberá desencriptar el tráfico SSL, de las aplicaciones web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío.
- En los modos puente (bridge) o sniffer, la solución deberá poder desencriptar el tráfico SSL para inspección, sin terminar o cambiar la conexión HTTPS.
- La solución deberá tener la capacidad de proteger aplicaciones web que incluyan el contenido de servicios web (xml). La protección XML deberá contar con mecanismos automatizados de aprendizaje, similares a los de la protección de aplicaciones web.
- La solución deberá soportar la conmutación de datos por error o failover.
- La solución deberá soportar las opciones fail-open y fail-closed.
- Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones ip maliciosas, botnets y sitios de phishing.
- Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.

- Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
- Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).
- Bloquear solicitudes de acceso basado en el país de origen de la conexión.
- Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial
- Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.
- Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http.
- Inspeccionar las peticiones y respuestas http.
- Tener la habilidad de decodificar datos a su mínima expresión a partir de diferentes sistemas de encoding Web y validarla.
- Validar todos los tipos de datos ingresados, incluyento URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.

## 4. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Estas aplicaciones deben ser suplidas y manejadas exclusivamente por el proveedor.
- El proveedor debe proporcionar entrenamiento de la solución al personal de la SIB.
- 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 el Web Application Firewall (WAF) en la institución una vez sea revisado y aprobado por el personal de la SIB.

## 5. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- El suplidor debe realizar la implementación de la solución con las configuraciones y políticas de protección de las aplicaciones web de la Superintendencia de Bancos
- Propuesta de Web Application Firewall (WAF)
- Plan de trabajo de Implementación de un Web Application Firewall (WAF)
- El suplidor debe de entregar el equipo Web Application Firewall (WAF) de la Superintendencia de Bancos en funcionamiento

## 6. PERFIL PROFESIONAL

- El proveedor de Web Application Firewall (WAF) 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 Web Application Firewall (WAF) para empresa, independientes de la seguridad de la industria.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta Web Application Firewall (WAF)

- El proveedor debe ser capaz de atender todo el alcance de los requisitos del appliance de seguridad, incluido el rendimiento, velocidad de conexión desde la pequeña oficina hasta el centro de datos en un único dispositivo de hardware.

## 8. IMPLEMENTACIÓN DE HERRAMIENTA DE CLASIFICACIÓN DE LA INFORMACIÓN

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Herramienta de Clasificación de la información | UN | 650 |
| B | 3 Años de Soporte y Mantenimiento | UN | 1 |

### 1. PLANTEAMIENTO DE LA NECESIDAD

En vista de que la protección de datos no estructurados es uno de los mayores desafíos organizativos y que cualquier empleado de la institución puede enviar un correo electrónico, crear un documento o subir un archivo es necesario que nuestras políticas de seguridad protejan la información confidencial de lo contrario se expone la institución a riesgo.
Se necesita una herramienta que permita clasificar, proteger y compartir de forma segura la información de la organización.

### 1. OBJETIVOS

#### 1.1. Objetivo General

Implementar una herramienta para la clasificación de la información en la Superintendencia de Bancos.

### 1.2. Objetivos Específicos

- Descubrir datos en reposo en red
- Clasificar automáticamente los archivos en función de contenido y contexto
- Proteger archivos con cifrado y opciones de remediación
- Analizar resultados para entender mejor tu información

## 2. FUNCIONALIDADES DE LA HERRAMIENTA DE CLASIFICACIÓN DE LA INFORMACIÓN

**Descubrimiento de datos**

- La solución debe de descubrir e identificar grandes volúmenes de datos, almacenados en las instalaciones, escanear recursos compartidos de red, SharePoint (en las instalaciones y en línea).

**Clasificación automática**

- Ejecutar exploraciones programadas para clasificar automáticamente los archivos en función de varios factores, incluidos las propiedades / atributos del archivo, el contenido y / o los metadatos.

**Protección de archivos**

- Cifrar automáticamente los archivos según las reglas de sensibilidad de datos. Esta capa adicional de protección. se puede agregar en función de los detalles del propio archivo o de su ubicación.

**Inventario de datos**

- Recopilar información del archivo durante los análisis, incluidas las propiedades del archivo, la clasificación (antes y después del análisis), y controles de acceso. Esto le permite ver cuáles son sus datos, dónde están y quién tiene acceso a ellos.

**Análisis de datos**

- Analizar los resultados a través del panel integrado o sus propias herramientas de análisis para minimizar los datos en riesgo. Supervisar las actividades de clasificación y optimizar las políticas de identificación de datos y las soluciones de almacenamiento de datos.

**Remediación**

- La solución debe tener la capacidad de poner en cuarentena los archivos almacenados de forma inadecuada, marcar los archivos para su seguimiento y realizar acciones basadas en los resultados de la exploración. Esto puede incluir la actualización de políticas de seguridad de sus usuarios en el tratamiento de datos sensibles.

**Habilitación de seguridad**

- Mejorar la capacidad de DLP, ERM y otras soluciones de seguridad para aplicar los adecuados controles basados en la clasificación.

## 3. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Las 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 de implementar la herramienta de clasificación de la información una vez sea revisado y aprobado por el personal de la Superintendencia de Bancos (SIB).

## 4 PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- Propuesta de la herramienta clasificación de la información
- El proveedor debe proporcionar entrenamiento de la solución.
- Plan de trabajo de Implementación de herramienta clasificación de la información.
- Herramienta de clasificación de la información de la Superintendencia de Bancos en funcionamiento.
- El suplidor debe realizar la implementación de la solución con las configuraciones y políticas de clasificación de la información de la Superintendencia de Bancos.

## 5. PERFIL PROFESIONAL

- El proveedor de la herramienta 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 de clasificación de la información para empresa, independientes de la seguridad de la industria.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta de clasificación de la información.

- El proveedor debe ser capaz de atender todo el alcance de los requisitos de herramienta de clasificación de la información

## 9. ADQUISICIÓN E IMPLEMENTACIÓN DE UNA HERRAMIENTA DE GESTIÓN DE CUENTAS PRIVILEGIADAS

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Herramienta de Gestión Cuentas privilegiadas | UN | 120 |
| B | 3 Años de Soporte y Mantenimiento | UN | 1 |

## 1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente la Superintendencia de Bancos (SIB) necesita una herramienta que nos ayude a centralizar, controlar y auditar el acceso a las cuentas de administrador dotadas de una importante carga de información sensible. En vista de que las organizaciones se enfrentan hoy en día a enormes desafíos de seguridad y crecientes presiones regulatorias que hacen mandatorio controlar y supervisar a sus usuarios privilegiados. Las cuentas de superusuario, como las de los administradores de bases de datos (DBAs), administradores de sistemas operativos (root), aplicaciones e infraestructura, implica un alto riesgo de destrucción, pérdida o robo de información confidencial de la empresa, daños malintencionados, multas o compromisos de la red.
Se necesita una herramienta que nos ayude a la gestión de identidades privilegiadas, restringir los permisos y garantizar que el acceso sea exclusivamente a los recursos específicos que cada perfil requiere para sus funciones, realizar seguimiento de las

acciones generadas sobre los servidores con información crítica, grabar las sesiones, validar la legitimidad de los usuarios que realicen acciones sobre la infraestructura crítica y evitar las contraseñas compartidas a través de medios no seguros y sin control.

## 2. OBJETIVOS

### 2.1. Objetivo General

Implementar una herramienta de administración de cuentas privilegiadas de la Superintendencia de Bancos.

### 2.2. Objetivos Específicos

- Almacenar contraseñas seguras
- Trazar acciones ejecutadas sobre los servidores
- Evitar suplantación de usuarios
- Permitir compartir contraseñas de forma segura
- Hacer segregación de perfiles

## 3. FUNCIONALIDADES REQUERIDAS

Plataformas/dispositivos/sistemas operativos soportados

- Capacidad de administrar cuentas privilegiadas de diferentes orígenes o plataformas.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de Windows, Linux, entre otros.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de MS SQL Server; MySqlServer, Postgres, ORACLE.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas basadas en AD.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de dispositivos de red (CISCO y otros).
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de aplicaciones (Web y Cliente Servidor).
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de SaaS/websites/web interfaces.
- La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de Virtual Servers (VmWare y HiperV)

- La solución propuesta deberá ser capaz de soportar cualquier dispositivo de red mediante conexión SSH.
- La solución propuesta deberá ser capaz de soportar cualquier repositorio de datos mediante conexión ODBC.
- La solución no debe tener un límite de cuentas privilegiadas que pueda administrar.
- La solución propuesta deberá ser capaz de permitir a través de un administrador definir y agregar cuentas privilegiadas
- La solución propuesta deberá ser capaz de soportar dispositivos-plataformas "out of the box".
- La solución propuesta deberá proporcionar mecanismos para organizar las cuentas privilegiadas.
- La solución propuesta deberá ser capaz de detectar automáticamente nuevos dispositivos Laptops o PCs Windows, Servicios Windows (Windows Services), Scheduled Tasks, IIS Service Accounts, etc. para su administración en la solución.

Administración de la Solución

- La solución propuesta deberá permitir una administración centralizada.
- La solución propuesta deberá incluir en su documentación técnica las versiones de sistemas operativos de desktops soportados y/o browsers y versiones soportados por la solución para la interfaz de administración.
- Si la solución propuesta utiliza una base de datos como back-end, esta base de datos deberá ser autoadministrable, es decir, no se requerirá la participación de un administrador de base de datos DBA para la implementación, respaldo, recuperación o hardening de la base de datos.
- La solución propuesta deberá permitir denegar a administradores poder acceder, ver password o aprobar solicitudes de requerimientos de password.
- La solución propuesta deberá tener la capacidad de aprovisionar usuarios en forma automática a partir de un Active Directory o LDAP, para así contar con un aprovisionamiento automático y transparente de cuentas que reflejen los cambios en dichos directorios.
- La solución propuesta deberá tener la capacidad de manejar los controles de acceso basado en roles mediante la administración de grupos de usuarios de Active Directory o LDAP.
- La solución propuesta deberá tener la capacidad de ejecutar operaciones en forma masiva (bulk operations) sobre las cuentas privilegiadas

- La solución propuesta deberá tener la capacidad de soportar lenguaje español e inglés en sus interfaces de usuario
- La solución propuesta deberá soportar la administración centralizada de usuarios en diferentes zonas horarias

Arquitectura de la solución

- La solución propuesta podrá ser instalada en servidores virtuales
- La solución propuesta deberá ser escalable mediante un diseño modular para adaptarse a crecimientos de utilización o de inclusión de más plataformas.

Alta disponibilidad/Redundancia

- La solución propuesta deberá tener la capacidad de permitir una alta disponibilidad (24x7x365) y redundancia en caso de fallas en hardware, aplicación, falla de datos o desastres catastróficos.

Disaster Recovery

- La solución propuesta deberá ser capaz de manejar la pérdida de conectividad con el repositorio central de passwords.
- La solución propuesta deberá ser capaz de soportar a sistemas replicados en datacenters de Disaster Recovery ubicados en diferentes localidades geográficas.

Network architecture support

- La solución propuesta deberá ser capaz de soportar una arquitectura de red distribuida donde los diferentes segmentos necesitan ser soportados desde una localidad central.
- La solución propuesta deberá contar dentro de su documentación, un diagrama técnico de la arquitectura de la solución incluyendo comunicaciones de red y reglas que permitan la administración de plataformas-servidores remotos conectados a través de un firewall (por ejemplo, servidores en una DMZ, localidades remotas, etc.
- La solución propuesta deberá contar dentro de su documentación con una lista de todos los puertos y protocolos utilizados por la solución, así como una descripción del uso de cada uno de estos puertos y protocolos.

Seguridad de la Aplicación

- La solución propuesta deberá tener la capacidad de integrarse con métodos empresariales de autenticación, por ejemplo, LDAP, Windows SSO, PKI y mecanismos propios de autenticación.
- La solución propuesta deberá tener la capacidad de encriptar todos los datos.
- La solución propuesta deberá tener la capacidad de encriptar la comunicación entre todos los componentes de la solución, incluyendo los componentes que residan en un mismo servidor.
- La solución propuesta deberá tener la capacidad de contar con respaldos encriptados.
- Separación de responsabilidades- La solución propuesta deberá tener la capacidad de permitir que ciertos administradores no puedan visualizar los passwords que son controlados por otros departamentos de la compañía, por ejemplo, que administradores de Windows Server no puedan visualizar los passwords ni accesos a instancias de bases de datos SQL Server.
- Plataforma segura - La solución propuesta deberá ser capaz de asegurar el repositorio de passwords (firewall, hardening, control remoto limitado y restringido, etc.)
- La solución propuesta deberá ser capaz de contar con un repositorio seguro y a prueba de falsificaciones (tamper-proof) de credenciales privilegiadas, políticas, grabaciones, entitlements, registros de auditorías, etc.
- La solución propuesta deberá contar con la capacidad de contener alguna credencial hard coded que no pueda ser asegurada/administrada dentro de la misma solución
- La solución propuesta deberá contar con certificaciones de terceros que tenga la solución (por ejemplo: Common Criteria, VerAfied, etc)

Integraciones

- La solución propuesta deberá contar con la capacidad de integrarse con sistemas de tickets tipo service desk.

- La solución propuesta deberá contar con la capacidad de verificar si existe un ticket válido y con el status requerido para extraer un password del repositorio.

- La solución propuesta deberá tener la capacidad de crear automáticamente un nuevo ticket cuando se solicita un password de una cuenta privilegiada.

- La solución propuesta deberá tener la capacidad de integrarse con el sistema de tickets para que cuando se genere un ticket de cierto tipo se pueda ligar a un workflow de aprobación.

Integración con sistemas tipo SIEM (Security Information Event Management)

- La solución propuesta deberá contar con la capacidad de integrarse con sistemas tipo SIEM.

- Identity Management/User Provisioning

- La solución propuesta deberá contar con la capacidad de integrarse con sistemas de Identity Management.

- La solución propuesta deberá contar con la capacidad de administrar y modificar automáticamente usuarios y grupos dentro del producto de acuerdo a cambios que sucedan en algún sistema externo de Identity Management.

  Integración LDAP/AD

  - La solución propuesta deberá tener la capacidad de integrarse con directorios LDAP/AD.

  - La solución propuesta deberá tener la capacidad de hacer búsquedas y controlar el acceso a passwords para nested global groups incluyendo múltiples forests, localidades geográficas, incluyendo búsquedas complejas en LDAP.

Integración con sistemas de manejo de vulnerabilidades

- La solución propuesta deberá tener la capacidad de integrarse con soluciones de manejo de vulnerabilidades para realizar escaneos automáticos y profundos.

Reportes/Auditoría /Assessment

- La solución propuesta debe tener la capacidad de mapear cuentas privilegiadas y cuentas personales de la organización con una herramienta stand alone.

- La solución propuesta debe tener la capacidad de descubrir e identificar fácilmente cuentas privilegiadas que no se adhieren a la política corporativa de passwords sin haber implementado aún una solución de manejo de cuentas privilegiadas.

- La solución propuesta deberá tener la capacidad de listar cuentas utilizadas para hacer login a servidores/Workstation en un periodo de tiempo determinado (por ejemplo, en el último trimestre), sin haber implementado aún un sistema de manejo de cuentas privilegiadas.

- La solución propuesta deberá tener la capacidad de mostrar en un quick view todas las actividades relativas a una cuenta privilegiada, como el release de un password o sesiones de administración utilizando dicha cuenta.

- La solución propuesta deberá tener la capacidad de generar todos los reportes de forma periódica, bajo demanda o en forma programada.

La solución propuesta deberá tener la capacidad de generar reportes detallados y programados con la siguiente información:

- Entitlements Reports
- Actividad de usuarios
- Inventario de cuentas privilegiadas
- Inventario de aplicaciones
- Reportes de Cumplimiento

La solución propuesta deberá tener la capacidad de exportar los reportes a los siguientes formatos

- Microsoft Excel
- CSV
- PDF

- La solución propuesta deberá tener la capacidad de generar reportes de todos los cambios administrativos en el sistema.

- La solución propuesta deberá tener la capacidad de generar un reporte de todos los accesos al sistema.

- La solución propuesta deberá tener la capacidad de generar un reporte de todos los checkouts de passwords y de usuarios que solicitan passwords.

- La solución propuesta deberá tener la capacidad de generar un reporte de intentos inválidos de login al sistema.

- La solución propuesta deberá tener la capacidad de generar un reporte de la verificación de valores de passwords

- La solución propuesta deberá tener la capacidad de reportar los cambios automáticos de passwords después del proceso de verificación de los mismos

- La solución propuesta deberá tener la capacidad de reportar reconciliaciones de passwords en un sistema o múltiples sistemas, reconciliación es la recuperación automática del sistema cuando un password ha sido cambiado por error en el dispositivo pero que no fue sincronizado con la solución

- La solución propuesta deberá tener la capacidad de generar reportes de passwords de sistemas que no cumplen la política a la cual pertenecen dichos sistemas.

- La solución propuesta deberá tener la capacidad de generar reportes por system id o por tipo de dispositivo dentro de una política.

- La solución propuesta deberá tener la capacidad de generar reportes sobre el status de los passwords

- La solución propuesta deberá tener la capacidad de personalizar reportes.

- La solución propuesta deberá tener la capacidad de restringir el acceso a los reportes de auditoría (y a la configuración de dichos reportes) solo para personal de auditoría.

- La solución propuesta deberá tener la capacidad de reproducir las sesiones grabadas para propósitos de análisis forense.

Soporte a workflows

- La solución propuesta deberá tener la capacidad de soportar controles duales, la solución debe soportar diferentes configuraciones de aprobaciones cuando por

ejemplo un usuario solicite un password. Esto debe incluir notificaciones automáticas vía email.

- La solución propuesta deberá tener la capacidad de que un usuario pueda solicitar el uso de una cuenta privilegiada para una fecha u hora futura.

- La solución propuesta deberá tener la capacidad de soportar procesos flexibles de workflows para designar múltiples aprobadores. Por ejemplo, se requieren dos o más aprobaciones antes de que el acceso sea autorizado.

- La solución propuesta deberá tener la capacidad de generar logs de los procesos de workflow y/o la habilidad de generar reportes o auditarlos.

System Password Management/Privileged Credential Management

Opciones de cambio de passwords

- La solución propuesta deberá tener la capacidad de cambiar passwords cada X días, meses, años.
- La solución propuesta deberá tener la capacidad de cambiar múltiples passwords en una sola vez para un solo sistema o sistemas agrupados bajo un solo criterio.
- La solución propuesta deberá tener la capacidad de cambiar un password o un grupo de passwords:
- De acuerdo a una política (cada x dias u 'on-demand')
- Cambios manuales efectuados por un usuario
- Automáticamente, cuando un password no ha sido sincronizado (falla en verificación)
- La solución propuesta deberá tener la capacidad de asignar passwords a un valor random.
- La solución propuesta deberá tener la capacidad de cambiar manualmente un password por un administrador en cualquier momento.
- La solución propuesta deberá tener la capacidad de cambiar automáticamente el valor de un password después de un tiempo especificado de un "chek out" del password

- La solución propuesta deberá tener la capacidad de cambiar automáticamente el password de una cuenta que acaba de ser definida en el sistema.

Soporte a verificación de passwords

- La solución propuesta deberá tener la capacidad de verificación automática del valor de un password en el sistema correspondiente.

- La solución propuesta deberá tener la capacidad de notificar automáticamente aquellos passwords que están "out of synch" con el sistema.

- La solución propuesta deberá tener la capacidad de reportar todos los passwords que están fuera de sincronía "out of sync".

Soporte a Reconciliación de Passwords

- La solución propuesta deberá tener la capacidad de automáticamente reconciliar passwords que se hayan detectado como "out of sync" o que se hayan perdido, sin utilizar herramientas externas de restauración.

- La solución propuesta deberá tener la capacidad de reconciliar passwords en un sistema, en múltiples o en todos los sistemas bajo el control del producto.

- La solución propuesta deberá tener la capacidad de reconciliar passwords de forma manual o bajo demanda.

Políticas de Contraseña (no heredadas del AD)

- La solución propuesta deberá tener la capacidad de configurar una longitud mínima de contraseña y complejidad para cuentas de super-usuarios de todos los sistemas.

- La solución propuesta deberá tener la capacidad de mantener el historial de contraseñas, ej. Las últimas tres contraseñas o por periodo de tiempo y proveer fácil acceso a ellas a través de la interfaz web del producto.

- La solución propuesta deberá tener la capacidad de administrar cuentas de super-usuario que han sido renombradas de su nombre por default.

- La solución propuesta deberá tener la capacidad de fortalecer la política de contraseña cuando las cuentas se cambian manualmente, así como cuando los sistemas cambian la contraseña aleatoriamente

- La solución propuesta deberá tener la capacidad de fortalecer x últimas únicas contraseñas (I.E. no repite los últimos x contraseñas).

- La solución propuesta deberá tener la capacidad de ofrecer contraseñas únicas por dispositivo.

- La solución propuesta deberá tener la capacidad de fortalecer las diferentes políticas por línea de negocio cuando el tipo de negocio es el mismo.

- La solución propuesta deberá tener la capacidad de establecer políticas unificadas para la administración de cuentas privilegiadas y monitoreo de sesiones.

Proceso de verificación de contraseña

- La solución propuesta deberá tener la capacidad de generar contraseñas "one time" como una opción de flujo de aprobación.

- La solución propuesta deberá tener la capacidad de enviar notificaciones vía correo electrónico u otros métodos de envío por tipos de actividad.

- La solución propuesta deberá tener la capacidad de verificar una contraseña para un período específico, ej. Horas y/o días.

- La solución propuesta deberá tener la capacidad de enviar notificaciones vía correo electrónico al usuario que solicitó la contraseña para indicarle que se aprobó su solicitud.

- La solución propuesta deberá tener la capacidad de enviar notificaciones vía correo electrónico a un usuario para avisarle sobre la expiración de una contraseña cuando la nueva contraseña no ha sido asignada (ej. La contraseña necesita ser cambiada manualmente).

- La solución propuesta deberá tener la capacidad de permitir exclusividad de recuperación de contraseña o múltiples usuarios verificando la misma contraseña para el mismo dispositivo en el mismo periodo.

Conexión a Sistemas Target

- La solución propuesta deberá tener la capacidad de soportar conexiones transparentes a un dispositivo target, sin la necesidad de ver o teclear la contraseña como parte de la conexión.

- La solución propuesta deberá tener la capacidad de soportar conexión directa a dispositivos Windows.

- La solución propuesta deberá tener la capacidad de soportar conexión directa a dispositivos UNIX/LINUX de administración (SSH).

- La solución propuesta deberá tener la capacidad de soporte dinámico para sistemas target adicionales que no son soportados "out of the box".

La solución propuesta deberá tener la capacidad de enviar correos electrónicos para lo siguiente:

- Accesos a Sistemas
- Cambios a Sistemas
- Uso de Contraseñas
- Solicitudes de aprobación de contraseña

Monitoreo/Grabación de Actividad Privilegiada

- La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas en: Windows, Virtual Servers, Linux, Ruteadores y Switches, Bases de Datos, Aplicaciones Web.

- La solución propuesta deberá tener en su documentación los protocolos soportados.

- La solución propuesta deberá tener la capacidad de extender para soportar cualquier aplicación o dispositivo de conexión para monitorear y habilitar autenticación única privilegiada.

- La solución propuesta deberá tener la capacidad de contar con métodos de monitoreo.

Arquitectura y Seguridad

- La solución propuesta deberá tener la capacidad de no requerir que se instalen agentes en los dispositivos target.

- La solución propuesta deberá tener la capacidad de que la grabación de la sesión no impacte el rendimiento del dispositivo target.

- La solución propuesta deberá tener la capacidad de no requerir cambios en la topología de red con la finalidad de asegurar que todas las sesiones privilegiadas son controladas por la solución.

- La solución propuesta deberá tener en su documentación los puertos de Firewall que se necesitan abrir con la finalidad de almacenar las grabaciones al servidor central.

- La solución propuesta deberá tener la capacidad de que para una solución que requiere instalación de agente, se pueda prevenir a los administradores que deshabiliten la grabación de la sesión.

- La solución propuesta deberá tener la capacidad de aplicar segregación de deberes, ej. Permitir a los administradores de Windows solo ver las sesiones Windows.

- Grabación de la sesión - La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas y las almacena de forma segura en un repositorio encriptado y a prueba de falsificaciones.

- La solución propuesta deberá tener la capacidad de soportar autenticación fuerte para acceso remoto privilegiado, ej. El usuario root.

- La solución propuesta deberá tener la capacidad de que las conexiones remotas pueden ejecutarse sin tener que exponer las credenciales privilegiadas aún manteniendo un control de acceso estricto.

- La solución propuesta deberá tener la capacidad de forzar control de acceso a dispositivos target.

Funcionalidad de la Solución

- La solución propuesta deberá tener la capacidad de administración de cuentas privilegiadas y el control se encuentra dentro de la solución de monitoreo de sesiones.

- La solución propuesta deberá tener la capacidad de monitorear las actividades privilegiadas cuando la administración de una de las cuentas privilegiadas no está en el radar.

- La solución propuesta deberá tener la capacidad de soportar auditoría correlacionada y unificada para la administración y actividad de cuentas compartidas y cuentas privilegiadas.

- La solución propuesta deberá tener la capacidad de asegurar responsabilidad personal cuando se abre una sesión privilegiada con una cuenta compartida.

- La solución propuesta deberá tener la capacidad de crear reglas basadas en políticas y flujos de trabajo flexibles para inicializar la grabación de sesiones.

- La solución propuesta deberá tener la capacidad de ayudar a investigar causas raíz y análisis forense.

- Conexiones Remotas Seguras (ej. Acceso remoto a terceros) - La solución propuesta deberá tener la capacidad de soportar conexiones remotas seguras a los dispositivos target (para escenarios cuando se conectan externamente de la empresa al centro de datos de la empresa - la solución no debe confiar en la SSL/VPN de la empresa para permitir conexiones remotas seguras).

- La solución propuesta deberá tener la capacidad de aislar los sistemas target de las vulnerabilidades potenciales de equipos de escritorio ej. Infectados por malware, ataques persistentes avanzados, etc.

- La solución propuesta deberá tener la capacidad de actuar como una caja servidor seguro de paso.

- La solución propuesta deberá tener la capacidad de monitorear, controlar y grabar a Administradores de base de datos.

- La solución propuesta deberá tener la capacidad de no impactar en el rendimiento de la base de datos.

- La solución propuesta deberá tener la capacidad de fortalecer la autenticación y flujos de acceso para iniciar una sesión privilegiada.

- La solución propuesta deberá tener la capacidad de monitorear, controlar y grabar administradores de Hypervisor.

- La solución propuesta deberá tener la capacidad de fortalecer la autenticación y flujos de acceso para iniciar una sesión privilegiada en ESX/ hosts de ESXi, administración de herramientas (vCenter) y máquinas invitado.

- La solución propuesta deberá tener la capacidad de hacerse búsquedas de comandos privilegiados dentro de las grabaciones de video.

- La solución propuesta deberá tener la capacidad de integrarse a sistemas de Ticketing/HelDesk/Change Management y permitir la validación de tickets antes de establecer la sesión.

- La solución propuesta deberá tener la capacidad de ver las sesiones en vivo/tiempo real del monitoreo de sesiones.

- La solución propuesta deberá tener la capacidad de intervenir y/o terminar remotamente una sesión en tiempo real cuando se ejecuta actividad sospechosa.

- La solución propuesta deberá tener la capacidad de que las grabaciones de sesiones y las actividades de sesiones granular puedan ser vista en productos SIEM.

- La solución propuesta deberá tener la capacidad de proveer bastos colores y una gran resolución de grabación de video o solo un intervalo de imagen (blanco y negro) snapshots.

- La solución propuesta deberá tener la capacidad de comprimir las sesiones y sin impactar en la calidad de video.

Grabación de sesiones en línea SSH y SSH Proxy

- La solución propuesta deberá tener la capacidad de proveer administradores (Unix/Linux) con una interfaz CLI para iniciar la grabación de sesiones privilegiadas.

- La solución propuesta deberá tener la capacidad de ofrecer grabaciones keystroke de todas las sesiones privilegiadas.

- La solución propuesta deberá tener la capacidad de permitir a administradores UNIX/LINUX iniciar sesiones desde clientes SSH (IE, PuTTY).

- La solución propuesta deberá tener la capacidad de ofrecer aprovisionamiento automático de cuentas del Directorio Activo en sistemas UNIX.

Administración de Llaves SSH

- La solución propuesta deberá tener la capacidad de contar con un método para detectar llaves SSH pares, llaves huérfanas y relaciones de confianza en la organización.

- La solución propuesta deberá tener la capacidad de poder reportar status de llaves SSH e identificar aquellas llaves que no cumplan con la política.

- La solución propuesta deberá tener la capacidad de almacenar de forma segura y controlar el acceso a las llaves privadas SSH.

- La solución propuesta deberá tener la capacidad de permitir la automatización de rotación de llaves.

- La solución propuesta deberá tener la capacidad de administrar y resguardar las llaves usadas en aplicaciones.

- La solución propuesta deberá tener la capacidad de reportar el uso de las llaves SSH privadas.

- La solución propuesta deberá tener la capacidad de almacenar y administrar las llaves SSH dentro de la misma infraestructura que administra y almacena las contraseñas privilegiadas.

Análisis Proactivo de Amenazas

- La solución propuesta deberá tener la capacidad de ofrecer análisis inteligente para detectar actividad sospechosa para cuentas privilegiadas.

- La solución propuesta deberá tener la capacidad de reportar comportamiento anormal de cuentas privilegiadas - basado en algoritmos de adopción y comportamiento - orientado a soluciones SIEM.

- La solución propuesta deberá tener la capacidad de generar notificaciones de uso excesivo y uso fuera de horario de cuentas privilegiadas.

- La solución propuesta deberá tener la capacidad de detectar si una cuenta privilegiada es usada en una maquina target sin una previa solicitud de acceso.

## 4. REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- Las 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 proporcionar entrenamiento de la solución al personal de la SIB.

- El proveedor debe de implementar la herramienta de cuentas privilegiadas una vez sea revisado y aprobado por el personal de la Superintendencia de Bancos (SIB).

## 5. PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- El suplidor debe realizar la implementación de la solución con las configuraciones y políticas de protección de la gestión de cuentas privilegiadas de la Superintendencia de Bancos
- Propuesta de plataforma de herramienta de gestión de cuentas privilegiadas
- Plan de trabajo de Implementación de plataforma
- Herramienta de la Superintendencia de Bancos en funcionamiento

## 6. PERFIL PROFESIONAL

- El proveedor de la herramienta 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 en herramienta de cuenta privilegiada, independientes de la seguridad de la industria.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta de cuentas privilegiadas

# 10. IMPLEMENTACIÓN DE UNA HERRAMIENTA DE SEGURIDAD DATA BASE FIREWALL

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Herramienta de Seguridad Database Firewall para 6 servidores de 4 cores (total 24 cores) | UN | 1 |
| B | 3 Años de Soporte y Mantenimiento Premium | UN | 1 |

## 1.PLANTEAMIENTO DE LA NECESIDAD

Actualmente la SIB necesita una herramienta que proteja las bases de datos de la institución, estas almacenan información extremadamente valiosa y confidencial, por eso una cantidad creciente de regulaciones de conformidad obligan a las organizaciones a

hacer auditorías del acceso a dicha información restringida y a protegerla de los ataques y del mal uso.
Se necesita una herramienta para evitar que personas no autorizadas tengan acceso al sistema, ya sea para obtener información, efectuar cambios mal intencionados que automatice las auditorías de las bases de datos, e identifiquen de inmediato los ataques, las actividades malintencionadas y el fraude.

## 2. OBJETIVOS

### 2.1 Objetivo General

Implementar una herramienta para la seguridad de base de datos en la Superintendencia de Bancos.

### 2.2 Objetivos Específicos

- Tener capacidad total de auditoria y de visibilidad del uso de información de las bases de datos.
- Monitorear las actividades y proteger las bases de datos en tiempo real.
- Evaluar las vulnerabilidades, administración de las configuraciones y clasificación de la información de las bases de datos.
- Inspeccionar y administrar los derechos de acceso de usuario a bases de datos restringidas.

**FUNCIONALIDADES DE LA HERRAMIENTA DE PROTECCIÓN DE BASE DE DATOS**

- La solución deberá contar con tecnología de auto-aprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo schemas, objetos, tablas; sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de un baseline de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.
- La solución deberá proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.
- La solución deberá generar reportes y tendencias en tiempo real, así como permitir la modificación de los mismos.

- La solución deberá contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.
- La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.
- La solución deberá funcionar independiente a la activación de la auditoría nativa de la base de datos.
- La solución deberá ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.
- El repositorio para el registro de la actividad en el appliance, no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.
- La solución deberá ser capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.
- La solución deberá realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:
    - Cuestiones de configuración de la base de datos tales como nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas.

    - Cuestiones de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.

- La solución deberá de poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.
- La solución deberá tener la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.
- La solución deberá proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.
- La solución deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y Control de cambios.

- La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.
- La solución deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, links, stored procedures, entre otros.
- La solución deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.
- La solución deberá tener capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.
- La solución deberá proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.
- La solución deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:

    - Número de registros a regresar por la consulta (SQL Query)
    - Número de registros afectados
    - Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada)
    - Acceso a datos marcados como sensibles
    - Base de Datos, Schema, Instancia, Tabla y Columna accesada
    - Estado de autenticación de la sesión
    - Usuario y/o Grupo de Usuarios de Base de Datos conectado
    - Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares)
    - Logins, Logouts, Queries
    - IPs de origen y destino
    - Nombre de Host origen, Usuario firmado en el Host origen
    - Aplicación usada para la conexión a la base de datos
    - Tiempo de respuesta/procesamiento del query
    - Errores en el manejador de SQL
    - Número de ocurrencias en intervalos de tiempo definidos
    - Por operaciones básicas (Select, Insert, Update, Delete)

- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export)
- Por Stored Procedure o Function utilizada
- Si existe ticket asignado de cambios
- Hora del Día

- La solución deberá identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, ésta actividad no deberá implicar la modificación de la aplicación y/o de la base de datos.
- La solución debe posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.
- La solución deberá asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.
- La solución deberá proteger contra ataques SQL y no-SQL (como buffer overflow).
- La solución deberá correlacionar actividad en base de datos con actividad de aplicaciones web para entender detalladamente como los usuarios están accesando datos privilegiados sin necesidad de alterar la aplicación web.

Considerados de emergencia para potenciales violaciones de la información que incluyan, enunciativa mas no limitativamente:

- Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
- Acceso a datos inusual para cierta hora del día.
- Acceso a datos desde una ubicación (física) desconocida.
- Acceso a datos utilizando aplicaciones/herramientas no autorizadas.

- La solución debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.
- La solución debe tener facilidades de Archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP).
- La solución deberá contar con Políticas, Reportes, Análisis de Vulnerabilidades, Alertas, Objetos y Transacciones Sensibles; preidentificadas y preconfiguradas para trabajar con las siguientes plataformas empresariales: Oracle EBS, Peoplesoft, SAP.
- La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.
- La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:

- Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
- Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa.
- Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.
- Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar API's.
- Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL ó al momento de hacer login a las bases de datos.
- La solución debe permitir el manejo de alarmas y notificaciones –en tiempo real– para los eventos de correlación mencionados anteriormente.

- La solución debe tener la capacidad de monitorear aplicaciones web en la misma solución, ofreciendo una visibilidad, seguridad y control desde el usuario web hasta la base de datos.
- La solución deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas, para lo cual deberá presentar la documentación respectiva en el descubrimiento de las mismas.
- La solución deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo.

El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:

• Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
• Deberá incluir una lista preconfigurada y detallada de las firmas de ataque.
• Deberá permitir la modificación o adición de firmas por el administrador.
• Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
• Deberá detectar ataques conocidos en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor web y ataques a nivel de aplicación.

- La solución deberá soportar Gateway clúster a nivel de los agentes de monitoreo de Bases de Datos, es decir que los agentes estarán asignados a un Gateway y podrán moverse automáticamente o manualmente según sea

el caso sin necesidad de volver a registrar el agente con el Gateway o realizar alguna acción en el servidor en el cual se encuentra instalado el agente.

- La solución debe proporcionar un proceso de instalación, actualización y gestión de cambios centralizada, segura y ágil para los Agentes; la cual debe proporcionar una visión completa de todas las actualizaciones disponibles para los componentes de la solución de protección de Bases de Datos.
- La solución deberá notificar cuando se encuentre disponible una nueva versión de Agente.
- El despliegue y la instalación centralizada de parches y actualizaciones a componentes solo deberá ser realizada por usuarios con los privilegios necesarios y administradores de la herramienta.
- La solución deberá proporcionar información del tráfico enviado de los Agentes a los Gateways, identificando actividades de Bases de Datos que no son necesarias monitorear; permitiendo a los administradores de la solución generar reglas de exclusión para reducir el consumo de recursos en el servidor.
- La solución deberá contar con la opción de reducir el tráfico entre la comunicación entre el Agente y el Gateway utilizando métodos de compresión de datos.
- La solución deberá proporcionar la opción de enmascarar la información personal que se despliega a través de la interfaz de administración, además deberá contar con la opción de desenmascarar esta información dependiendo de los privilegios de cada usuario.
- Los diferentes componentes de seguridad de los aplicativos Web, DB y Sistemas de Archivos distribuidos en red deberán de administrarse a través de una consola centralizada.
- Los equipos que realicen el monitoreo deben de tener la capacidad de ejecutar simultáneamente los componentes de seguridad DB, Web y de Archivos dentro del mismo equipo.
- La consola centralizada deberá de ser el único punto de contacto, administración, control, análisis y reporteo para las diferentes soluciones e infraestructura de seguridad en aplicaciones Web, Bases de Datos y Sistemas de Archivo de Red.

La solución deberá soportar ser desplegada o implementada en línea como un puente o bridge transparente (capa 2 del Modelo OSI, las interfaces no requieren de una dirección IP y debe soportar bypass/ failopen/ failclose configurable tanto para fallas de hardware como software), como un proxy transparente o un proxy inverso (según se requiera), o como un analizador no en línea o un non-inline sniffer / monitor, a través de puertos Mirror o SPAN. Deberá también:

• En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.

• En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.
• Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas. Las acciones deberán incluir la habilidad para terminar las solicitudes y respuestas, bloquear la sesión TCP, bloquear el usuario de la aplicación, o bloquear la dirección IP.
• Respecto de ataques particularmente destructivos, la solución deberá ser capaz de bloquear la dirección IP por un periodo de tiempo configurable.
• En modo analizador de paquetes o sniffer, la solución deberá ser capaz de enviar un paquete TCP RST a ambos extremos de la conexión.
Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo, pero no tomar acción alguna.

- La solución deberá soportar el volumen de tráfico y deberá tener una latencia sub-milisegundo (< 1ms), para no impactar el desempeño de las aplicaciones.
- La solución deberá tener como límites operativos una capacidad mínima por appliance de 500/1000/2000/5000/10000 Mbps de tráfico inspeccionado.
- La solución deberá soportar opciones de conectividad física como 1Gb Ethernet en UTP o Fibra Óptica tipo SX, así como conectividad 1Gb en modos SR o LR.
- Las interfaces de conectividad a la red deberán de ser modulares para tener la posibilidad de hacer cambios de medio como por ejemplo Cobre UTP a Fibra Óptica y viceversa, sin necesidad de cambiar el appliance.

**REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR**

- Estas aplicaciones deben ser suplidas y manejadas exclusivamente por el proveedor.
- El proveedor debe proporcionar entrenamiento 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 herramienta de seguridad para la base de datos en la institución una vez sea revisado y aprobado por el personal de la SIB.

**PRINCIPALES ENTREGABLES**

A modo macro se detallan los principales entregables esperados:

- El suplidor debe realizar la implementación de la solución con las configuraciones y políticas de protección de las bases de datos de la Superintendencia de Bancos
- Propuesta de herramienta de protección para las bases de datos
- Plan de trabajo de Implementación de la herramienta de protección para las bases de datos
- Herramienta de protección de las bases de datos de la Superintendencia de Bancos implementada con las políticas institucionales y en funcionamiento

**PERFIL PROFESIONAL**

- El proveedor de la herramienta 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 herramientas para la protección de base de datos para empresa, independientes de la seguridad de la industria.

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

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta de seguridad de base de datos

## 11. HERRAMIENTA PARA ESCANEO DE VULNERABILIDADES POR 3 AÑOS

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Herramienta escaneo de Vulnerabilidades y cumplimiento para 512 hosts | UN | 1 |
| B | 3 Años Mantenimiento y Soporte | UN | 1 |

## 1. PLANTEAMIENTO DE LA NECESIDAD

Actualmente se 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 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 como también reparar cualquier imprevisto con rapidez y facilidad, incluso hasta fallas de software, parches faltantes, malware y configuraciones erróneas.

## 2. OBJETIVOS

### 2.1 Objetivo General

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

### 2.2 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 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”.

**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 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 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)

- El 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.

- 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 soluciones de bóveda digitales de credenciales 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 hosts 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 vía 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 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 7, Windows 10, Windows 2008, Windows 2012, Windows 2016, 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 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 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.

- El 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 vez 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. También debe admitirse la importación de una lista de IP contenidas en un archivo fuente.

- 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 realizar la auditoría de cumplimiento basada en agentes y sin agentes 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.

  - 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.

  - El producto debe proporcionar la auditoría de los principales sistemas operativos Unix / Linux para la configuración de seguridad y configuración de aplicativos instalados.

  - El producto debe proporcionar auditoria de bases de datos para la configuración de seguridad y configuraciones.

  - El producto debe proporcionar auditoria de aplicaciones para la configuración de seguridad y configuración.

  - El producto debe proporcionar auditoria de infraestructura de red o equipos de comunicaciones, para su endurecimiento de seguridad y prácticas recomendadas de configuración.

  - El producto debe proporcionar auditoria de paquetes antivirus específicos por: instalación, últimas actualizaciones y el estado de arranque del producto.

  - El producto debe proporcionar verificación de la información de identificación personal (PII) y otros contenidos sensibles o sensitivos.

  - El producto debe permitir que las plantillas utilizadas con políticas de auditoría puedan ser personalizables según las necesidades específicas de la organización.

  - 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).

- 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.

## 5 PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- El suplidor debe realizar la implementación de la solución con las configuraciones adecuadas para realizar el escaneo de vulnerabilidades de la infraestructura de la Superintendencia de Bancos
- 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

## 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.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de herramienta de escaneo de vulnerabilidades.

## 12. GESTIÓN Y CORRELACIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM)

| ÍTEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| A | Herramienta de Gestión y correlación de eventos e Información de seguridad (SIEM) | UN | 1 |
| B | 3 Años de Soporte, Mantenimiento y Garantía | UN | 1 |

## 1. PLANTEAMIENTO DE LA NECESIDAD

La Superintendencia de Bancos de la República Dominicana (SIB) está interesada en adquirir una solución de Gestión y Correlación de Eventos e Incidentes de Seguridad (SIEM) para mejorar su infraestructura de seguridad de información y así agregar valor para la protección de la confidencialidad, integridad y disponibilidad de la información de la institución.

Los componentes de la infraestructura tecnológica, las diferentes aplicaciones, sistemas de bases de datos y componentes de seguridad y de comunicaciones, generan una gran cantidad de eventos de seguridad en múltiples ubicaciones dentro de la red de la Superintendencia de Bancos. La gestión centralizada y correlación de los eventos e información de seguridad generados por estos elementos permite tener una mejor visibilidad y control de la plataforma tecnológica de la SIB.

## 2.OBJETIVOS

### 2.1 Objetivo General

Adquirir una solución de Gestión y Correlación de Eventos e Información (SIEM) de Seguridad que permita obtener una visión holística de la seguridad de la Tecnología de Información y Comunicaciones de la Superintendencia de Bancos.

### 2.2 Objetivos Específicos

- Obtener una vista holística de la seguridad de la infraestructura de TIC de la SIB.
- Consolidación y gestión de logs provenientes de distintas fuentes de datos.
- Correlacionar los eventos de las distintas fuentes de datos para convertirlos en información útil para la institución.
- Generar alertas y notificar a los responsables de la solución de incidentes.
- Convertir los datos de los eventos en gráficos de información que permitan identificar patrones o actividades que no corresponden a un patrón.
- Generar reportes que se adapten a los procesos de gobierno, seguridad y auditoría.
- Almacenar a largo plazo datos históricos de eventos para facilitar la correlación a través del tiempo y la investigación forense de cualquier violación de seguridad.

## 3 FUNCIONALIDADES DE SIEM

- La solución deberá incluir un sistema de respuesta a incidentes basado orientado a CSIRT (Computer Security Incident Response Teams) permitiendo tener una solución escalable.

- El sistema permite la definición de reglas de correlación de eventos, estableciendo la identificación de incidentes a nivel de red mediante reglas predefinidas para la correlación de eventos en diferentes dispositivos de red, a partir de estas reglas crear nuevas reglas para adaptarlas a las necesidades e identificar de forma automática las alteraciones de la red, aislando proactivamente incidentes o alteraciones de forma rápida y confiable.

- El sistema debe incluir reglas de correlación preconfiguradas y parametrizables para ataques/riegos/fallas comunes tales como:

    - Ataques de fuerza bruta.
    - Actividades sospechosas de logins por sistemas WEB
    - Actividad multicasting sospechosa
    - Ataques de reconocimiento haciendo escaneo de puertos por HTTP o HTTPS, ya sea a partir de eventos o flujos.
    - Gran cantidad de requerimientos HTTP no estándares.
    - Cantidad inusual de conexiones a una Base de Datos.
    - Múltiples logins fallidos desde una misma estación de trabajo.
    - Intentos fallidos de login de forma intensa.
    - Patrones de gusanos informáticos (Ej: W32.Blaster, SQL, Scanning, etc.)
    - Vulnerabilidades conocidas (SSH)
    - Cuentas de Windows creadas y eliminadas en menos de X horas (Ej; 24 horas)
    - No reinicio de servidores Windows
    - Malware Trojan
    - Ataques DoS

- Las reglas pre-configuradas deberán ser actualizadas por el fabricante y deberán basarse en los ataques, riesgos y fallas más comunes. Los datos de inteligencia de amenazas se pueden integrar en forma de listas de observación, reglas de correlación y consultas de forma que aumenten la tasa de éxito de la detección temprana de fallas.

El sistema deberá permitir recolectar eventos de mínimo las siguientes fuentes **y/o formatos:**

- Syslog, Syslog NG
- SNMP O SNMP TRAPS
- Formatted log files
- Comma/tab/space delimited, other
- ODBC y/o conexión hacia otras bases de datos remotas.
- Windows event logging API
- Plataformas de Seguridad (Firewalls, seguridad endpoints, web gateways)
- Equipos de red de datos
- Dispositivos comunicaciones, Ips, NetFlow.
- Otros

- El sistema debe almacenar los logs en su formato original, firmados, comprimidos y cifrados de forma centralizada. Debe tener capacidad de almacenar al menos 3 años para fines de análisis histórico.
- El sistema debe tener la capacidad de almacenar mínimo 3 meses de retención de logs en crudo disponibles en línea.
- El sistema debe ofrecer correlación en tiempo real, permitiendo gestionar las amenazas, rastrear y analizar la progresión de un ataque entre componentes y sistemas y, para el monitoreo de la actividad del usuario, rastrear y analizar la actividad de un usuario en todas las aplicaciones o rastrear y analizar una serie de transacciones relacionadas o eventos de acceso a datos. Debe establecer relaciones entre mensajes o eventos generados por dispositivos, sistemas o aplicaciones, en función de características tales como fuente, destino, protocolo o tipo de evento.

- El sistema debe permitir el mantenimiento preventivo y correctivo y tareas externas, tales como backups, backups programados, y opcionalmente inventario on-line o lanzamiento de escaneos.

- El sistema debe permitir tareas generales como: normalizar, priorizar, recolectar y, evaluar el riesgo.

- El sistema debe permitir el envío de alertas en tiempo real.

- El sistema en el "Dashboard" debe permitir observar las fuentes de logs por nombre de dispositivo.

- El sistema debe estar compuesto por funciones o módulos de correlación de eventos de logs, y eventos de seguridad.

- La interface del sistema debe permitir profundizar en cualquier elemento de datos con sólo un clic en el "Dashboard", con tanto detalle como sea necesario sin la necesidad de ninguna clase de solicitud SQL y sin requerir cambiar las interfaces o páginas.

- El monitoreo debe realizarse con alertas de criticidad, que podrán observarse mediante aplicaciones gráficas, dashboard configurable, estadísticas, cantidad de incidentes, top de alertas, entre otros.

- El sistema debe permitir la exportación de documentos de auditoría de seguridad, análisis de riesgos y controles de seguridad de aplicación.

- Métricas e indicadores presentados y formalizados para el cumplimiento de mínimo las normas ISO 2700X

- El sistema debe incluir las funcionalidades de monitoreo, análisis y respuesta de eventos e incidentes de seguridad.

- El sistema debe poder funcionar con agentes en la fuente de datos, cuando a ello hubiere lugar, de acuerdo al monitoreo de cada dispositivo.

- El sistema debe permitirle crear “conectores” para el nuevo hardware o software que se agregue como fuentes de datos al sistema.

- El sistema debe contar con una interface Web GUI compatible con navegadores estándares tales como Internet Explorer, Edge, Google Chrome, Firefox/Mozilla, entre otros.

- El sistema debe permitir la generación de reportes de procesamiento, repositorio y visualización a través de diferentes formatos: PDF Adobe o Excel o HTML.

- El sistema debe proveer una base predefinida de reportes estándar que permitan su aprovechamiento desde el inicio de la puesta en producción.

- El sistema deberá proveer reportes de auditoria pre-construidos basados en leyes de cumplimiento como mínimo en la norma ISO 2700X.

- Los reportes se deberán poder enviar por correo electrónico.

- El servicio deberá ser capaz de integrarse con Active Directory.

- El sistema debe permitir la integración a sistemas de análisis de vulnerabilidades para permitir utilizar esta información en los reportes, en la correlación y en la identificación de los riesgos.

- El sistema deberá estar orientado a recolección de registros de eventos para operaciones de seguridad y de cumplimiento de regulaciones mínimo en el estándar ISO 2700X.

- La solución debe demostrar capacidad de custodia de los registros de eventos, es decir, que se guarden de manera segura, confiable e inalterable y puedan ser datos adecuados para evidencia digital.

- El sistema podrá usar agentes externos en los dispositivos a monitorear, cuando a ello hubiere lugar.

- El sistema deberá ser escalable y soportar crecimiento de dispositivos, así como flujo de registros de eventos.

- El sistema debe incluir reglas de correlación sobre las mejores prácticas que existen en el mercado.

- Deberá manejar definiciones de vulnerabilidades de los dispositivos integrados a la solución.

- Las alertas generadas por el sistema deberán poderse enviar en **mínimo** los siguientes formatos:

    - Generación de un archivo de Texto
    - Envío de una trama SNMP
    - Envío de un Correo electrónico por SMTP
    - Reenvío de mensajes de syslog a un dispositivo externo
    - Ejecución de un comando
    - Asignación de una Tarea

- El sistema deberá poder exportar los datos en formato estándar para uso con otras herramientas mínimo CSV
- El sistema deberá permitir agrupar los dispositivos monitoreados para la facilidad de uso.
- El sistema deberá permitir el uso de roles y redes para el acceso a los recursos de la herramienta de los usuarios.
- El sistema deberá ser capaz de determinar el comportamiento de los sistemas monitoreados para generar referencias base y aprender con el tiempo de dichos comportamientos.
- Debe soportar de forma nativa la recolección de registros de eventos desde aplicaciones/dispositivos de seguridad, sistemas operativos, bases de datos y elementos de red
- Deberá contar con un módulo de análisis forense en donde se pueda ver los datos históricos y/o en tiempo real.
- La base de datos debe estar incluida en el precio de la solución y se espera que sea auto gestionado para no incurrir en costos y tiempos de DBA´s para su mantenimiento preventivo y correctivo.
- Integración con soluciones de DLP (Data Lost Preventions - Prevención de pérdida de datos) propias y de otros fabricantes.
- La solución ofertada deberá proveerse y ser configurada en un esquema de “alta disponibilidad” (High Availability) en modo activo-pasivo para el componente de correlacionador de eventos.
- Conectividad: El proveedor deberá suministrar todos los cables, módulos y accesorios requeridos, en caso de ser físico, para la implementación del sistema, asegurándose que el appliance sea compatible con todos los componentes y

elementos con que interactúa en el lugar de ubicación y configurar las herramientas de administración ofrecidas.

- La solución debe permitir conexiones cifradas desde y hacia los sensores interconectados.
- El sensor debe tener la capacidad de procesar información en tiempo real y enviarla al sistema central mediante comunicación segura (cifrada).

- Se debe realizar la retroalimentación de buenas prácticas en instalación, configuración, operación y administración del sistema de correlación de eventos - SIEM.

## 4 REQUERIMIENTOS DE LOS SERVICIOS A CONTRATAR

- La infraestructura tecnológica adquirida debe ser entregada, instalada, configurada, probada y puesta en funcionamiento acorde a los requerimientos de la Superintendencia de Bancos.

- Luego de finalizada la entrega y/o instalación el proveedor debe realizar las pruebas de funcionamiento respectivas para la infraestructura tecnológica y equipos de cómputo, así mismo entregará un documento técnico que especifique lo anterior y las pruebas realizadas.

- El proveedor deberá integrar la solución de SIEM acorde a los requerimientos de la SIB y buenas prácticas en implementación de la solución.

- 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 al personal de la SIB
  .
- EL proveedor debe implementar la plataforma de SIEM de la institución una vez sea revisado y aprobado por el personal de la Superintendencia de Bancos (SIB).

## 5 PRINCIPALES ENTREGABLES

A modo macro se detallan los principales entregables esperados:

- El suplidor debe realizar la implementación de la solución con las configuraciones y políticas de protección de la infraestructura tecnológica de la Superintendencia de Bancos.
- Propuesta de SIEM
- Plan de trabajo de Implementación de un SIEM
- El suplidor debe de entregar el equipo SIEM de la Superintendencia de Bancos en funcionamiento

## 6 PERFIL PROFESIONAL:

- El proveedor del SIEM 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 soluciones SIEM para empresas basada en datos independientes de la seguridad de la industria.

- El proveedor debe ser capaz de atender todo el alcance de los requisitos del SIEM.

- El suplidor debe proporcionar evidencia de posición de liderazgo de la solución año tras año en el Cuadrante Mágico de Gartner para soluciones de SIEM

- 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 SIEM (Security Information and Event Management)

# 13. ROBUSTECIMIENTO DE PLATAFORMA BLADE

## PLANTEAMIENTO DE LA NECESIDAD

Como parte de la estrategia de mejoramiento de las facilidades tecnológicas de la (SIB) Superintendencia de Bancos de la República Dominicana, el departamento de (TyO) Tecnología y Operaciones ha determinado las necesidades a ser suplidas mediante los bienes y servicios detallados en este documento.

**DESCRIPCIÓN DE LOS BIENES Y ESPECIFICACIONES TÉCNICAS**

En la actualidad la institución cuenta con una plataforma de consolidación donde residen los servicios críticos de la misma. Conscientes de la necesidad de mitigar cualquier riesgo de falla de esta plataforma la institución desea tener a su disposición el hardware necesario que sirva de espejo al ambiente actual a fin de suplir las funcionalidades y servicios que actualmente se consumen.

Nuestra plataforma de consolidación cuenta con un chasis Blade Synergy Frame 12000, con servidores BL 480 Gen10, con equipos de red tanto para la SAN como para LAN. La adquisición de los equipos homólogos a esta plataforma persigue un ambiente resiliente ante fallos no planificados.

Esta plataforma debe contar con los siguientes componentes técnicos:

| ITEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| **PLATAFORMA BLADE** | | | |
| A | Chasis para servidores Blades | UN | 1 |
| B | Servidores Blade Consolidación | UN | 2 |
| C | Servidores Blade Servicios | UN | 8 |
| D | Almacenamiento All Flash | UN | 1 |
| E | Enrutador de servicios integrados | UN | 4 |
| F | Conectividad LAN | UN | 4 |
| G | Gaveta para Expansion 3PAR 7200 con sus Cables + 12 DISCOS DE 800GB SSD | UN | 1 |

**DETALLE DE LAS ESPECIFICACIONES TÉCNICAS**

**PLATAFORMA BLADE**

a. **(1)** Chasis para servidores Blades – Synergy Frame 12000
    1. Capacidad para al menos 16 nodos con facilidad de crecimiento y configurados como un ambiente consolidado.
    2. Consola de administración y monitoreo consolidada para toda la plataforma.
    3. Soporte por lo menos de 4 fabrics y/o PCI Express con I/O redundantes (Ethernet, Fibre Channel, InfiniBand, iSCSI, SAS, etc.) de forma simultánea.
    4. Power Supply y abanicos inteligentes y redundantes, completos e instalados
    5. Consola de configuración con administración remota y con capacidad de integración al Directorio Activo
    6. Segregación de accesos

7. Gestión KVM remoto vía IP
8. Interfaz independiente de management
9. Kit de instalación para Rack
10. Conectividad a la LAN
    i. Al menos 4 puertos redundantes de 10GbE
    ii. Al menos 4 Puertos de 40GbE o similares
11. Integración con la SAN
12. Segmentación de trafico
13. Casos de éxito para virtualización
14. Soporte y Garantía por 3 Años

b. Servidor Blade Consolidación
    a. **(2)** Servidores Blades Instalados y Configurados
        i. Al menos 2 procesadores Intel Xeon E5 v4
            1. Mínimo 2.2 Ghz
            2. No menos de 24 Cores x CPU
        ii. Aceleradores de carga con NVMe SSD y memoria persistente
        iii. Conectores redundantes a la LAN (4 Puertos 10Gb) y la SAN(FC)
        iv. Memorias DDR4 con funcionalidades iguales o similares a:
            1. ECC avanzada
            2. Memory Mirroring
            3. Memory Online Spare Mode (Rank Spare Mode)
            4. 1.5 TB instalada en cada servidor, con capacidad de crecimiento
        v. Capacidad de al menos 4 módulos de interconexión a la red al menos 10Gb para un total de 40Gb de interconexión a la LAN.
        vi. Controladora SATA integrada tipo FIO
        vii. Controladora de arreglo de discos integrada tipo 1G FIO
        viii. Almacenamiento de al menos 16 GB SD o Discos de estado sólido redundantes
        ix. Soporte y Garantía por 3 Años

Servidor Blade Servicios

c. **(8)** Servidores Blades Instalados y Configurados
    a. No más 1 procesadores Intel Xeon E5 v4
        i. Mínimo 1.7 Ghz
        ii. No menos de 6 Cores x CPU
    b. Aceleradores de carga con NVMe SSD y memoria persistente
    c. Conectores redundantes a la LAN 10Gb y la SAN(FC)
    d. Memorias DDR4 con funcionalidades iguales o similares a:
        i. ECC avanzada
        ii. Memory Mirroring
        iii. Memory Online Spare Mode (Rank Spare Mode)
        iv. 768 GB instalada en cada servidor, con capacidad de crecimiento

e. Capacidad de al menos 4 módulos de interconexión a la red al menos 10Gb para un total de 40Gb de interconexión a la LAN.
f. Controladora SATA integrada tipo FIO
g. Controladora de arreglo de discos integrada tipo 1G FIO
h. Almacenamiento de al menos 16 GB SD o Discos de estado sólido redundantes
i. Soporte y Garantía por 3 Años

d. Almacenamiento de Contingencia (Solución All Flash)
    a. **(1)** Tecnologia de almacenamiento Electrónica (Flash)
    b. Controladora redundante
        i. Capacidad al menos 2 puertos 10GBASE-T
        ii. Al menos 4 Puertos Fibra Canal 16Gb
    c. Al menos 100TB Usables
        i. No menos de 80TB RAW
    d. Software para:
        i. Gestión
        ii. Compresión
        iii. Deduplicacion
        iv. Clonación
        v. Mantenimiento
        vi. Monitoreo
        vii. Analítica
    e. Soporte y Garantía por 3 Años
        i. Actualización de Software
        ii. Remplazo de piezas
        iii. Upgrade de productos
    f. Capacitación del Personal
        i. Entrenamiento para 4 personas
    g. Instalación y Configuración

e. **(4)** Enrutador de servicios integrados (Router)
    a. Compliant Standards: ANSI T1.101, IEEE 802.1Q, IEEE 802.1ag, IEEE 802.3, IEEE 802.3ah, ITU-T G.823, ITU-T G.824. RMON, SNMP, Telnet
    b. characteristics: Access Control List (ACL) support, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), wall mountable, IPFIX, IPv6 support, NetFlow, Quality of Service (QoS), RADIUS support, Syslog support, VLAN support, VPN support
    c. Addressing protocol: BGP, DVMRP, RIP-1, RIP-2, policy-based routing (PBR), static IPv4 routing, static IPv6 routing, EIGRP, GRE, IGMPv3, IPv4-to-IPv6 Multicast, IS-IS, OSPF, PIM-SM, PIM-SSM
    d. RAM: 4 GB (installed) / 16 GB (max) - DDR3 SDRAM
    e. Flash memory: 4 GB (installed) / 16 GB (max)
    f. Interface: Ethernet 10Base-T/100Base-TX/1000Base-T, auxiliary, console

g. Connector type: 4 pin USB Type A, RJ-45, SFP (mini-GBIC), mini-USB Type B
h. IOS IP Base
i. Protocolos de VoIP
j. Soporte para SRST ( Survivable Remote Site Telephony)
k. Configuración de Alta Disponibilidad
l. Capacidad de configuración de Site Primario / Site Remoto (Fail Over / Fail Back), tanto para los servicios de datos como los servicios de Voz IP
m. Instalación y configuración
n. Soporte y garantía por 3 años

f. Conectividad LAN
   a. **(4)** Switches con 24 puertos de por lo menos 10GbE
   b. Stackwise support
   c. D-Access support
   d. Throughput de 480 Gbps
   e. Arquitectura CPU x86
   f. Soporte para ejecutar contenedores
   g. NSF/SSO
   h. Transferencia de control por debajo de los 50ms
   i. Soporte para UADP 2.0
   j. Manejo de IOS XE, NETCONF, RESTCONF, YANG
   k. Soporte para AES-256
   l. Integración de SUDI
   m. Capacidad de Co-located Border and Control Plane
   n. Manejo de Políticas con APIC-EM
   o. Integración de Flexible NetFlow (FNF)
   p. Dual Stack IPv4/IPv6
   q. PTP, IEEE 1588v2
   r. Cables e interfaz para configuración en nom-blocking Stack
   s. Instalación y configuración
   t. Soporte y garantía por 3 años

g. Gaveta de Expansión para 3PAR 7200
   a. Al menos 12 discos SSD
   b. No menos de 800 GB por disco
   c. Cables para conectividad al equipo
   d. Configuración
   e. Soporte y Garantía

**SERVICIOS DE CONSULTORÍA PARA IMPLEMENTACIÓN**

- Instalación y configuración
- Documentación de la Solución

- Capacitación para 6 personas. Especificar horas de capacitación. La capacitación debe ser orientada a la gestión de la solución, así como el primer nivel de soporte interno.

**DE LA CAPACITACIÓN**

El objetivo principal de la capacitación es facultar al personal interno para instalar, configurar, administrar, diagnosticar fallas o eventos y dar soporte de primer nivel a la solución. No debe confundirse con la tradicional "Transferencia de Conocimiento", ya que esta no suele perseguir validar el nivel requerido.

**DE LAS COTIZACIONES**

Las cotizaciones deben ser redactadas en idioma español. Los documentos complementarios y literatura impresa que proporcione el ofertante podrán estar escritos en idioma inglés.

Las cotizaciones deberán incluir los siguientes documentos:

- Lista de precios de los bienes ofertados incluyendo los impuestos que aplican a dichos bienes
- Tiempo de entrega
- Tiempo de Implementación
- Nombres de Clientes con solución similar instalada
- Números de parte de los equipos y del soporte
- Especificaciones Técnicas
- Certificación del oferente en los productos ofrecidos
- Carta del fabricante autorizando al oferente a comercializar los bienes ofertados en el territorio de la República Dominicana.
- Descuentos aplicados y el origen de estos.

## 14. SERVICIO DE COLOCACIÓN PARA DATACENTER (COLLOCATION) POR 3 AÑOS

**PLANTEAMIENTO DE LA NECESIDAD**

Como parte de la estrategia de mejoramiento de las facilidades tecnológicas de la (SIB) Superintendencia de Bancos de la República Dominicana, el departamento de (TyO) Tecnología y Operaciones ha determinado las necesidades a ser suplidas mediante los bienes y servicios detallados en este documento.

**DESCRIPCIÓN DE LOS BIENES Y ESPECIFICACIONES TÉCNICAS**

En cumplimiento a las mejores prácticas de la industria y con el objetivo de dotar a la institución de los servicios necesarios para la continuidad de sus operaciones, estamos

solicitación la adquisición de los servicios de colocación de nuestros equipos de computación y procesamientos de datos. Dicho servicio fungirá con Sitio de Recuperación de Desastres (SRD) al integrarlos con los equipos tanto de data, procesamiento y comunicación de la institución.

Para tales propósitos hemos identificado los siguientes elementos a ser adquiridos:

| ITEM | DESCRIPCIÓN | UNIDAD | CANTIDAD |
|---|---|---|---|
| **SERVICIO COLOCACIÓN PARA DATACENTER** | | | |
| 1 | Gabinete de 42U | UN | 1 |
| 2 | Alimentación Eléctrica Redundante | UN | 2 |

**DETALLE DE LAS ESPECIFICACIONES TÉCNICAS**

**SERVICIO COLOCACIÓN PARA DATACENTER**

1. Gabinete de 42U
    a. Gabinete de 42U's
    b. profundidad estándar
    c. puertas y paneles laterales
    d. Puertas frontal y trasera con cerradura
    e. Disponibilidad de expansión
    f. 4 postes verticales interiores con orificios cuadrados sin rosca
    g. Ventilación y climatización
    h. Cumplimiento de requisitos PCI-DSS
    i. Detallar costos de:
        i. Instalación / configuración
        ii. Renta mensual
    j. Contratación de Servicios por 3 años

2. Alimentación Eléctrica Redundante
    f. Circuito de energía redundante de 208v AC (A + B) @ 30 Amperes
    g. Sistema de monitoreo y control para los circuitos eléctricos
    h. Detallar costos de:
        i. Instalación / configuración
        ii. Renta mensual
    i. Contratación de Servicios por 3 años

**DEL AMBIENTE PROPUESTO**

El propósito principal es conseguir expandir el ambiente actual para interconectar con una localidad remota. De esta forma se logrará un ambiente robusto, estable,

y resiliente. Las facilidades ofertas deberán ofrecer las siguientes facilidades con la intención de limitar el crecimiento de nuestras necesidades futuras:

- Unidades de precisión redundantes
- Sistemas de prevención y mitigación de incendios
- Organización “Hot Aisle / Cold Aisle”
- Diversidad de agentes de enfriamiento
- Sistemas de monitoreo y control para los sistemas ambientales
- Sensores de temperatura, humedad
- Escalerillas para la corrida de cableado eléctrico y de datos en cobre y fibra óptica
- Garantías contractuales respecto de energía, humedad, temperatura y soporte técnico
- Servicios de Manos Remotas
- Servicios de Manos Inteligentes

**De las cotizaciones**

Las cotizaciones deben ser redactadas en idioma español. Los documentos complementarios y literatura impresa que proporcione el ofertante podrán estar escritos en idioma inglés.

Las cotizaciones deberán incluir los siguientes documentos:

- Lista de precios de los bienes ofertados incluyendo los impuestos que aplican a dichos bienes
- Tiempo de entrega
- Tiempo de Implementación
- Nombres de Clientes con solución similar instalada
- Números de parte de los equipos y del soporte
- Especificaciones Técnicas
- Certificación del oferente en los productos ofrecidos
- Carta del fabricante autorizando al oferente a comercializar los bienes ofertados en el territorio de la República Dominicana.
- Descuentos aplicados y el origen de los mismos.

## 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-001/2019
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

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.**

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-001/2019**

## 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. Formulario de Entrega de Muestra **(SNCC.F.056)**.
3. 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.
4. Resumen de experiencia del Personal Profesional propuesto **(SNCC.D.045)**: Certificación de los técnicos.
5. Resumen de Experiencia del Oferente en Servicios Similares (de igual magnitud). . **(SNCC.D.048)**
6. **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-001/2019**

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 | COMPUTADORA DE ESCRITORIO (DESKTOPS) | 90 | 1 MES |
| 2 | COMPUTADORA DE ESCRITORIO ESPECIALES (DESKTOP) | 10 | 1 MES |
| 3 | COMPUTADORA PORTÁTIL (LAPTOP) | 50 | 1 MES |
| 4 | ACTUALIZACIÓN PLATAFORMA DE FIREWALLS CHECKPOINT | 4 | 3 MESES |
| 5 | IMPLEMENTACIÓN SOLUCIÓN DE AUTENTICACIÓN DE DOBLE FACTOR CON TOKEN | 350 | 2 MESES |
| 6 | IMPLEMENTACIÓN DE UN (INSTRUSION DETECTION PREVENTION SYSTEMS) (IDPS) | 2 | 3 MESES |
| 7 | IMPLEMENTACIÓN DE UN EQUIPO WEB APPLICATION FIREWALL | 1 | 3 MESES |
| 8 | IMPLEMENTACIÓN DE HERRAMIENTA DE CLASIFICACIÓN DE LA INFORMACIÓN | 1 | 3 MESES |
| 9 | IMPLEMENTACIÓN DE UNA HERRAMIENTA DE CUENTAS PRIVILEGIADAS | 1 | 3 MESES |
| 10 | IMPLEMENTACIÓN DE UNA HERRAMIENTA DE SEGURIDAD DATA BASE FIREWALL | 1 | 3 MESES |
| 11 | HERRAMIENTA PARA ESCANEO DE VULNERABILIDADES POR 3 AÑOS | 1 | 3 MESES |
| 12 | GESTIÓN Y CORRELACIÓN DE EVENTOS DE INFORMACIÓN DE SEGURIDAD (SIEM) | 1 | 3 MESES |
| 13 | ROBUSTECIMIENTO DE PLATAFORMA BLADE | 1 | 2 MESES |
| 14 | SERVICIO DE COLOCACIÓN PARA DATACENTER (COLLOCATION) POR 3 AÑOS | 1 | 2 MESES |

### 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.