LICITACIÓN PÚBLICA DA No. 687-IGSS-2023

EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL (IGSS)

CONVOCA A TODAS LAS PERSONAS INDIVIDUALES O JURÍDICAS, NACIONALES O EXTRANJERAS INTERESADAS EN OFERTAR PARA LA:

ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD

REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-.

Las personas individuales o jurídicas, nacionales o extranjeras interesadas en participar podrán adquirir los Documentos de Licitación, en forma gratuita, por medio electrónico, descargándolos de Guatecompras (www.guatecompras.gt), registrado bajo el Número de Operación Guatecompras (NOG) **20911777,** o a través de la dirección de Internet del Instituto (www.igssgt.org).

La recepción de ofertas se llevará a cabo el **06 de noviembre de 2023**, a las **10:00 horas** (hora límite 10:30), en Salones Los Volcanes, ubicados en la 7ª. Avenida 22-72 Zona 1, segundo nivel de Oficinas Centrales del Instituto y la apertura de plicas se realizará en el mismo lugar, después de concluida la recepción de ofertas.

De no llevarse a cabo la recepción en el lugar antes indicado, se colocará un aviso tanto en el portal de GUATECOMPRAS, como en el lugar señalado inicialmente, con la nueva ubicación.

Guatemala, septiembre de 2023.

INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL
-IGSS-

DOCUMENTOS DE LICITACIÓN
DA No. 687-IGSS-2023

ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD

REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-.

Guatemala, septiembre de 2023

7ª. Avenida 22-72, zona 1, Centro Cívico Guatemala, C. A. PBX: 2412-1224, ext. 1238

CONTENIDO DE LOS DOCUMENTOS DE LICITACIÓN

1. TERMINOLOGÍA

1.1 ANEXO (S)

Apartado de estos Documentos de Licitación identificados en el numeral 6 del contenido de los Documentos de Licitación que se agregan y forman parte del presente proceso.

1.2 AUTORIDAD ADMINISTRATIVA SUPERIOR

El Gerente del Instituto Guatemalteco de Seguridad Social -IGSS- o Subgerente por delegación de funciones. (Artículo 15 del Decreto Número 295 del Congreso de la República de Guatemala, Ley Orgánica del Instituto Guatemalteco de Seguridad Social y Artículo 9 del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado).

1.3 AUTORIDAD SUPERIOR

Junta Directiva del Instituto Guatemalteco de Seguridad Social -IGSS-. (Artículo 3 del Decreto Número 295 del Congreso de la República de Guatemala, Ley Orgánica del Instituto Guatemalteco de Seguridad Social y Artículo 9 del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado).

1.4 BASES DE LICITACIÓN

Apartado en el que se establecen los requisitos técnicos, financieros, legales y demás condiciones de la negociación, que conforme a la Ley deberán cumplir los oferentes para presentar sus ofertas según lo solicitado en el numeral 2. (Artículo 2 numeral 5 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.5 CONTRATISTA

Persona individual o jurídica, nacional o extranjera con quien se suscribe un contrato. (Artículo 2 numeral 7 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.6 CONTRATO

Es el instrumento legal, suscrito por el funcionario titular de la AUTORIDAD ADMINISTRATIVA SUPERIOR o el funcionario que esta Autoridad delegue, ambos del Instituto Guatemalteco de Seguridad Social -IGSS- y por el CONTRATISTA donde se estipulan los derechos y las obligaciones que rigen la ejecución de la negociación y las relaciones entre los mismos, cuyas condiciones surgen de todos los Documentos de Licitación, técnicos y legales que integran el proceso.

1.7 DEPARTAMENTO DE ABASTECIMIENTOS

Dependencia administrativa del Instituto Guatemalteco de Seguridad Social -IGSS- encargada de coordinar los procesos de compras, ubicada en la 7ª. Avenida 22-72 zona 1, tercer nivel, Oficinas Centrales del Instituto Guatemalteco de Seguridad Social -IGSS-. Teléfono: 2412-1224, extensiones: 1233 a la 1235, 1237 y 1239, con horario de atención al público de lunes a viernes de 8:00 a 16:00 horas.

1.8 DISPOSICIONES ESPECIALES

Apartado que contiene las características específicas, necesidades, estructura u objetivos adicionales que se requieren en el numeral 5, según el objeto de la negociación, utilizados para complementar las bases y especificaciones técnicas. (Artículo 2 numeral 10 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.9 EQUIPO (S)

Una (1) Solución Integrada de Ciberseguridad, el cual se ha definido con base a las especificaciones y características descritas en los Documentos de Licitación.

1.10 DOCUMENTOS DE LICITACIÓN

Agrupación de documentos que se integran por: BASES DE LICITACIÓN, Especificaciones Generales, Especificaciones Técnicas, DISPOSICIONES ESPECIALES y ANEXOS. (Artículos 18 y 20 del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado y Artículo 16 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.11 ESPECIFICACIONES GENERALES

Apartado en el cual se establecen los aspectos generales del objeto de la contratación de este proceso, identificados en el numeral 3. (Artículos 18 y 20 del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado).

1.12 ESPECIFICACIONES TÉCNICAS

Apartado en el que se establecen las características, requisitos, normas, exigencias o procedimientos de tipo técnico que debe reunir un producto, requeridos en el numeral 4. (Artículos 18 y 20 del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado y Artículo 2 numeral 12 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.13 FORMULARIO ELECTRÓNICO

Formulario generado electrónicamente a través del Sistema de Información de Contrataciones y Adquisiciones del Estado denominado GUATECOMPRAS, de uso obligatorio, el cual cuenta con los siguientes apartados: Datos del Proceso de Compra, Datos del Oferente, Datos de los Productos, Requisitos solicitados en las bases del Proceso, Anexos y Adjuntos Legales. (Artículo 24 Bis del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado).

1.14 GUATECOMPRAS

El Sistema de Información de Contrataciones y Adquisiciones del Estado denominado GUATECOMPRAS, es un sistema para la transparencia y la eficiencia de las adquisiciones públicas. Su consulta es pública, irrestricta y gratuita, y provee información en formatos electrónicos y de datos abiertos sobre los mecanismos y las disposiciones normadas en el Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado y Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado. (Artículo 4 Bis del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado y Artículo 4 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado). Su dirección en Internet es www.guatecompras.gt.

1.15 INSTITUTO

Instituto Guatemalteco de Seguridad Social -IGSS-, entidad autónoma con personalidad jurídica, patrimonio y funciones propias; goza de exoneración total de impuestos, contribuciones y arbitrios, establecidos o por establecerse. (Artículo 100 de la Constitución Política de la República de Guatemala). Oficinas Centrales ubicadas en la 7ª. Avenida, 22-72, zona 1, Centro Cívico, Guatemala. Sitio WEB: www.igssgt.org.

1.16 JUNTA

Junta de Licitación integrada con tres miembros titulares y dos miembros suplentes, nombrada por la AUTORIDAD SUPERIOR del INSTITUTO. (Artículos del 10 al 14 del Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado, Artículos 10 y 12 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado y normativa interna vigente del INSTITUTO).

1.17 LEY

Decreto Número 57-92 del Congreso de la República de Guatemala, Ley de Contrataciones del Estado. (Artículo 2 numeral 15 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.18 MODIFICACIÓN (ES)

Instrumento que modifica los presentes DOCUMENTOS DE LICITACIÓN. (Artículo 19 bis de la LEY).

1.19 OBJETO

ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD, REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-.

1.20 OFERENTE (S)

Persona individual o jurídica, nacional o extranjera que presenta una oferta. (Artículo 2 numeral 17 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.21 OFERTA

Propuesta presentada por cada OFERENTE para ejecutar el OBJETO de la contratación de este proceso.

1.22 PLICA (S)

Sobre cerrado y sellado, dentro del cual el OFERENTE presenta la documentación física y demás requerimientos y formalidades para el presente proceso. (Artículo 18 del Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado).

1.23 REGLAMENTO

Acuerdo Gubernativo Número 122-2016, Reglamento de la Ley de Contrataciones del Estado.

1.24 UNIDAD SOLICITANTE

Subgerencia de Tecnología, ubicada en 7ª Av. 22-72 zona 1, tercer nivel, Oficinas Centrales del Instituto Guatemalteco de Seguridad Social, ciudad de Guatemala, Teléfonos: 24121224 Extensiones 83196, 83255.

2. BASES DE LICITACIÓN

2.1 OBJETO DE LOS DOCUMENTOS DE LICITACIÓN

El presente proceso de Licitación tiene como objetivo recibir OFERTAS para la ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD, REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-; con fundamento en lo que establece la LEY, el REGLAMENTO; y de acuerdo con las condiciones y requerimientos establecidos en las BASES DE LICITACIÓN, ESPECIFICACIONES GENERALES, ESPECIFICACIONES TÉCNICAS, DISPOSICIONES ESPECIALES y ANEXOS de los presentes DOCUMENTOS DE LICITACIÓN. (Artículos 18, 19 y 20 de la LEY).

2.2 CRONOGRAMA DE ACTIVIDADES

	DESCRIPCIÓN	FECHA
2.2.1	Período para adquirir los DOCUMENTOS DE LICITACIÓN.	A partir de su publicación en GUATECOMPRAS, hasta el día 06 de noviembre de 2023.
2.2.2	Fecha y hora para inducción a interesados en ofertar el OBJETO de los DOCUMENTOS DE LICITACIÓN.	El día **27 de octubre de 2023, a las 10:00 horas.** La inducción se impartirá de forma virtual, por lo que los interesados deberán enviar un correo electrónico a la dirección deptoabastosigss@gmail.com a efecto de que se les envíe la invitación correspondiente.
2.2.3	Fecha, hora y dirección de las visitas	Los días **23 y 26 de octubre de 2023**, a las **10:00 horas** en la Subgerencia de Tecnología ubicada en la 7ª Av. 22-72 zona 1, tercer nivel, Oficinas Centrales del INSTITUTO.
2.2.4	Período para solicitud de aclaraciones sobre los DOCUMENTOS DE LICITACIÓN.	A partir de la publicación de la convocatoria en GUATECOMPRAS, hasta tres (3) días hábiles antes de la fecha establecida para presentar OFERTAS.
2.2.5	Período para respuestas de aclaraciones sobre los DOCUMENTOS DE LICITACIÓN.	A más tardar dos (2) días hábiles antes de la fecha fijada para presentar OFERTAS.
2.2.6	Período para la preparación del FORMULARIO ELECTRÓNICO.	La preparación del FORMULARIO ELECTRÓNICO puede elaborarse en GUATECOMPRAS desde el momento que se ha publicado el concurso hasta antes de la fecha y hora de recepción.
2.2.7	Lugar, dirección, fecha y hora para la recepción de OFERTAS.	En Salones Los Volcanes, ubicados en la 7ª. Avenida 22-72 zona 1, segundo nivel, Oficinas Centrales del INSTITUTO, el **día 06 de noviembre de 2023, a las 10:00** horas (hora límite **10:30**), transcurrido este plazo la JUNTA no recibirá ninguna OFERTA. De no llevarse a cabo la recepción en el lugar antes indicado, se colocará un aviso tanto en el portal de GUATECOMPRAS, como en el lugar señalado inicialmente, con la nueva ubicación.
2.2.8	Apertura de PLICAS.	Después de concluido el período de presentación y recepción de OFERTAS.

2.2.9	Plazo para adjudicar.	Hasta diez (10) días hábiles contados a partir del día siguiente de la fecha de recepción de OFERTAS. La JUNTA puede solicitar a la AUTORIDAD ADMINISTRATIVA SUPERIOR en forma justificada por única vez, prórroga para adjudicar la cual podrá ser por el mismo plazo o menor. (Artículos 33 de la LEY y 21 del REGLAMENTO) En caso que la JUNTA solicite la prórroga, esta deberá realizarla por lo menos dos (2) días hábiles anteriores al vencimiento del plazo establecido para la adjudicación. La AUTORIDAD ADMINISTRATIVA SUPERIOR deberá resolver lo procedente en un plazo de un (1) día hábil posterior a la recepción de la solicitud.

2.3 CONVOCATORIA A LICITAR Y OBTENCIÓN DE LOS DOCUMENTOS DE LICITACIÓN

La convocatoria a licitar se publicará en GUATECOMPRAS y una vez en el Diario Oficial. (Artículos 22 y 23 de la LEY y 17 del REGLAMENTO).

Los DOCUMENTOS DE LICITACIÓN serán puestos a disposición de los interesados en GUATECOMPRAS y en la dirección de Internet del INSTITUTO. (www.igssgt.org).

Los interesados en participar en el presente proceso podrán adquirir los DOCUMENTOS DE LICITACIÓN, en forma gratuita, por medio electrónico, descargándolos de GUATECOMPRAS, consultando el Número de Operación Guatecompras (NOG) **20911777.** (Artículo 22 de la LEY).

2.4 VISITA

Con la finalidad de evaluar el ambiente operativo donde deberá ser instalado el EQUIPO, los interesados deberán realizar la visita de acuerdo a lo establecido en el cronograma de actividades. Queda a criterio de los interesados definir en cuál de las dos fechas efectuará su visita. Dicha visita es **obligatoria.** De la misma, la UNIDAD SOLICITANTE, extenderá constancia de acuerdo al ANEXO 6.5 de los DOCUMENTOS DE LICITACIÓN.

2.5 PLAZO PARA SOLICITAR ACLARACIONES Y MODIFICACIONES DE LOS DOCUMENTOS DE LICITACIÓN

Los interesados podrán solicitar aclaraciones a través de GUATECOMPRAS, dentro del período establecido en el cronograma de actividades de los presentes DOCUMENTOS DE LICITACIÓN. El INSTITUTO aclarará o emitirá las MODIFICACIONES si correspondieran.

El INSTITUTO, en el curso de la presente Licitación y antes de la recepción de OFERTAS podrá emitir las MODIFICACIONES a los presentes DOCUMENTOS DE LICITACIÓN que crea convenientes, publicándolas en GUATECOMPRAS. (Artículo 19 bis de la LEY).

2.6 ELABORACIÓN DE LA OFERTA

Los OFERENTES deben realizar su propuesta, de acuerdo a lo estipulado en estos DOCUMENTOS DE LICITACIÓN, en caso de discrepancia en el contenido de los mismos prevalecerán en el siguiente orden: BASES DE LICITACIÓN, ESPECIFICACIONES

TÉCNICAS, DISPOSICIONES ESPECIALES y ESPECIFICACIONES GENERALES. (Artículo 16 del REGLAMENTO).

Los OFERENTES deben presentar los documentos requeridos en original y copia, en PLICAS separadas, rotuladas con la siguiente información del OFERENTE: Nombre, razón social o denominación social, dirección, números telefónicos y otros medios de comunicación, la identificación del proceso y la palabra original y copia según corresponda. La copia será puesta a disposición de los OFERENTES para consulta. (Artículo 19, numeral 4 de la LEY).

a) En idioma español, Se exceptúa manuales o documentación técnica.

b) Los documentos deben ser legibles, no deben contener enmiendas, borrones o correcciones, excepto que estas últimas, estén debidamente salvadas, como lo establece el Artículo 159 del Decreto Número 2-89 del Congreso de la República de Guatemala, Ley del Organismo Judicial y el Artículo 14 del Decreto Número 314 del Congreso de la República de Guatemala, Código de Notariado. Esta excepción no aplica para los Requisitos Fundamentales contenidos en el subnumeral 2.9 de los presentes DOCUMENTOS DE LICITACIÓN.

c) El Seguro de Caución de Sostenimiento de Oferta deberá ser entregado dentro de una bolsa de polietileno u otro material impermeable y transparente, que permita su resguardo y visualización, sin perforaciones, manchas, errores o correcciones.

d) Con excepción del Seguro de Caución de Sostenimiento de Oferta, todos los folios deben estar numerados en la parte inferior derecha, firmados por el Propietario, Representante Legal o Mandatario del OFERENTE, con índice del contenido y con los documentos ordenados de acuerdo a como se listan en el subnumeral 2.8 de los presentes DOCUMENTOS DE LICITACIÓN.

e) Cada OFERENTE podrá presentar una sola OFERTA. (Artículo 25 de la LEY).

f) El precio de la contratación se pactará como precio cerrado. (Artículo 7 segundo párrafo de la LEY y Artículo 2 numeral 23) del REGLAMENTO).

g) Los documentos que contiene la PLICA no serán devueltos.

h) La JUNTA no aceptará OFERTAS enviadas por correo electrónico, ni presentadas extemporáneamente. (Artículo 24 de la LEY).

2.7 FORMULARIO ELECTRÓNICO:

Los OFERENTES deberán acceder a GUATECOMPRAS a través del NOG **20911777,** ingresando los datos que correspondan y los parámetros establecidos en el ANEXO **6.1** Instructivo para el llenado de los Requisitos de las Bases en el FORMULARIO ELECTRÓNICO, dicho FORMULARIO ELECTRÓNICO, deberá ser impreso y firmado por el Propietario, Representante Legal o Mandatario según el caso.

La preparación del FORMULARIO ELECTRÓNICO puede iniciar desde el momento en que se ha publicado el concurso hasta antes de la fecha y hora de recepción de OFERTAS. En caso surjan dudas relacionadas con GUATECOMPRAS al momento de dicha elaboración,

las mismas deben ser resueltas por la Dirección General de Adquisiciones del Estado -DGAE-, comunicándose al número telefónico (502) 2374-2872.

2.7.1 OFERTA ECONÓMICA

Los OFERENTES al ingresar los datos que correspondan en la Oferta Económica contenida en el FORMULARIO ELECTRÓNICO, deben tomar en cuenta lo siguiente:

a) De acuerdo a lo que establecen los Artículos 25 y 25 Bis de la LEY, en ningún caso se permitirá a un compareciente la representación de más de un OFERENTE. Quien actúe por sí no puede participar representando a un tercero.

b) El Precio Unitario y el Monto Ofertado, deben ser expresados en quetzales, en números y decimales y el Monto Ofertado en letras, tal y como lo genera el sistema GUATECOMPRAS.

c) El Monto Ofertado debe incluir el Impuesto al Valor Agregado -IVA-, de acuerdo a lo que establece el Artículo 10 del Decreto Número 27-92 del Congreso de la República de Guatemala, Ley del Impuesto al Valor Agregado y Artículo 2 numeral 16) del REGLAMENTO.

d) El OFERENTE debe considerar en el Monto Ofertado, todos los costos en que incurra el OBJETO del presente proceso, de acuerdo a lo establecido en los presentes DOCUMENTOS DE LICITACIÓN. Razón por la cual el INSTITUTO no reconocerá suma alguna por este concepto, ni efectuará reembolsos de ninguna naturaleza.

2.8 LISTADO DE DOCUMENTOS QUE DEBERÁ CONTENER LA PLICA

a) FORMULARIO ELECTRÓNICO generado electrónicamente a través del sistema GUATECOMPRAS, de uso obligatorio el cual deberá ser llenado, impreso y firmado por el Propietario, Representante Legal o Mandatario, según el caso, mismo que deberá ser incorporado en los documentos que conforman la PLICA. (Artículo 24 Bis de la LEY).

   El código de autenticidad del FORMULARIO ELECTRÓNICO, deberá coincidir con el creado en el sistema GUATECOMPRAS, el cual será verificado por la JUNTA a través de GUATECOMPRAS.

   Este requisito no será necesario presentarlo en caso de realizarse una Adquisición Directa por Ausencia de Ofertas, sin embargo, los OFERENTES deben presentar una propuesta económica que contenga información detallada de su OFERTA conforme lo indicado en el subnumeral 2.7.1 de los presentes DOCUMENTOS DE LICITACIÓN.

b) Original del Seguro de Caución de Sostenimiento de Oferta, de conformidad a los Artículos 3 literal b), 106 y 109 del Decreto Número 25-2010 del Congreso de la República de Guatemala, Ley de la Actividad Aseguradora y Artículo 64 de la LEY y de acuerdo al subnumeral 2.23.1 de los presentes DOCUMENTOS DE LICITACIÓN.

c) Certificación original de autenticidad emitida por la entidad Afianzadora que otorgó el Seguro de Caución de Sostenimiento de Oferta, en donde conste que el seguro fue emitido en cumplimiento al Decreto Número 25-2010 del Congreso de la República de

Guatemala, Ley de la Actividad Aseguradora y que el firmante de la póliza posee las facultades y competencias respectivas. (Artículo 59 del REGLAMENTO).

d) Declaración Jurada contenida en Acta Notarial, en donde conste lo siguiente:

d.1) Que (nombre del OFERENTE) no es deudor moroso del Estado ni de las entidades a las que se refiere el Artículo 1 de la Ley de Contrataciones del Estado.

d.2) Que conoce las penas relacionadas a la comisión del delito de Pacto Colusorio en las Adquisiciones Públicas establecidas en el Artículo 25 Bis de la Ley de Contrataciones del Estado, así como las penas y demás disposiciones contenidas en el Capítulo III del Título XIII del Decreto Número 17-73 del Congreso de la República de Guatemala, Código Penal.

d.3) Que (nombre del OFERENTE) no está comprendido en ninguna de las prohibiciones que establece el Artículo 80 de la Ley de Contrataciones del Estado.

d.4) Que leyó, estudió, aceptó y se somete expresamente a cada una de las condiciones, requisitos y demás estipulaciones establecidas y exigidas en los DOCUMENTOS DE LICITACIÓN DA Número seiscientos ochenta y siete guion IGSS guion dos mil veintitrés (**DA No. 687-IGSS-2023**), aclaraciones y MODIFICACIONES si las hubiere.

d.5) Que no existe conflicto de interés entre (nombre del OFERENTE) y el Banco _____ que acredite la titularidad de sus cuentas bancarias (el nombre del banco debe coincidir con la entidad bancaria que emita la certificación solicitada en los DOCUMENTOS DE LICITACIÓN).

d.6) Que la presentación de esta OFERTA no implica derecho alguno para la adjudicación de lo requerido y garantiza la veracidad y exactitud de toda la información proporcionada. En caso de ser adjudicado se compromete a cumplir con el OBJETO del proceso de Licitación DA Número seiscientos ochenta y siete guion IGSS guion dos mil veintitrés (**DA No. 687-IGSS-2023**), y acepta que la JUNTA está en su derecho de rechazarla de no convenir a los intereses del INSTITUTO.

d.7) Que (Nombre del OFERENTE) tiene la capacidad de ejecutar el OBJETO y que asume las responsabilidades administrativas, civiles y penales que se deriven del mismo.

d.8) En caso de ser adjudicado, (nombre del OFERENTE), se compromete a mantener vigente el documento requerido en la subliteral g) del subnumeral 2.8 de los DOCUMENTOS DE LICITACIÓN. Asimismo, encontrarse solvente de los pagos correspondientes a las contribuciones patronales y de trabajadores ante el INSTITUTO, para la suscripción del CONTRATO.

d.9) Que el OBJETO ofertado cumple con las ESPECIFICACIONES GENERALES, ESPECIFICACIONES TÉCNICAS y DISPOSICIONES ESPECIALES, requeridas en los presentes DOCUMENTOS DE LICITACIÓN, entre otros, lo siguiente:

d.9.1) Que (nombre del OFERENTE) cuenta con oficinas locales ubicadas geográficamente en el territorio de Guatemala, y cuenta con al menos un centro de soporte regional, fuera del territorio nacional, para garantizar la continuidad de servicio en caso de problemas en territorio nacional.

d.9.2) Que (nombre del OFERENTE) incluyó dentro de su propuesta, el traslado de conocimiento de la implementación y puesta en producción de la Solución de acuerdo con lo indicado en las especificaciones técnicas del componente de capacitación.

d.9.3) Que el OBJETO deberá ser nuevo, sin uso y en perfecto estado de funcionamiento.

d.9.4) En caso de ser adjudicado, (nombre del OFERENTE), se compromete a dar una garantía de fábrica, con cobertura durante un periodo de **tres (3) años en sitio**, para los equipos y licenciamiento Ofertados; debiendo indicar, la descripción completa de los alcances, beneficios y limitaciones de la garantía ofrecida, para el EQUIPO.

d.9.5) Que todas las características del servicio de garantías ofrecidas se encuentran operativas en la República de Guatemala.

d.9.6) En caso de ser adjudicado, (nombre del OFERENTE), deberá incluir el derecho de actualización de nuevas versiones y soporte en línea durante el tiempo que dure la garantía.

d.9.7) Que en caso de ser adjudicado (nombre del OFERENTE) se compromete a reemplazar los EQUIPOS recibidos por el INSTITUTO por otros nuevos e iguales características a los ofertados en caso que se determine que los mismos tienen fallas de fábrica, sin costo alguno para el INSTITUTO, en un plazo máximo de treinta (30) días hábiles; contados a partir de la fecha del reclamo, debiendo instalarlos, configurarlos y dejarlos en operación, en el lugar de destino final.

Dicha declaración deberá ser emitida con un **máximo de treinta (30) días calendario** antes de la presentación de la OFERTA.

e) Solvencia Patronal extendida por el INSTITUTO a nombre del OFERENTE, con el pago operado al **30 de septiembre de 2023** o posterior, la cual deberá ser solicitada en línea, por el Propietario, Representante Legal o Mandatario, al Departamento de Cobro Administrativo, a través de la página de servicios electrónicos https://servicios.igssgt.org. La JUNTA deberá verificar la autenticidad de dicha solvencia.

f) Fotocopia legible legalizada de los documentos siguientes:

f.1) Si el OFERENTE es persona individual:

- Testimonio de la Escritura Pública de Mandato, si fuera el caso, debidamente inscrito en los registros correspondientes.

f.2) Si el OFERENTE es persona jurídica:

- Documento Personal de Identificación -DPI- vigente del Representante Legal o Mandatario.

- Testimonio de la Escritura Pública de Mandato, si fuera el caso, debidamente inscrito en los registros correspondientes.

En caso de ser extranjeros adjuntar fotocopia legible legalizada de pasaporte completo vigente.

f.3) Autorización otorgada al distribuidor por el titular o Representante Legal de la casa matriz donde tenga la representación comercial para ofrecer y comercializar el OBJETO.

g) Constancia Electrónica de inscripción y precalificación como proveedor del Estado que para el efecto emita el Registro General de Adquisiciones del Estado -RGAE-, en la que indique: que el OFERENTE se encuentra debidamente habilitado, que posee las especialidades de precalificación siguientes: Clase: 4651 “Venta de computadoras, equipo periférico y programas de informática”; y/o Clase: 4652 "Venta de equipo, partes y piezas electrónicas y de telecomunicaciones”; y/o Clase: 6202 “Consultoría de informática, telecomunicaciones, gestión de instalaciones informáticas y programación”; y/o Clase: 6209 “Otras actividades de tecnología de la información y de servicios informáticos” que corresponde con el OBJETO de la contratación, de conformidad con el catálogo de Especialidades del Registro General de Adquisiciones del Estado -RGAE-, asimismo debe contener la capacidad económica del OFERENTE cuyo monto máximo de contratación debe ser mayor a la OFERTA económica que presente. (Acuerdo Ministerial Número 563-2018 del Ministerio de Finanzas Públicas y Oficio Circular Número 03-2019 de la Dirección General de Adquisiciones del Estado -DGAE-).

   Dicha Constancia deberá ser emitida en un plazo no mayor de treinta (30) días anteriores a la fecha de la recepción de OFERTAS y apertura de PLICAS de la presente LICITACIÓN. La JUNTA verificará la autenticidad de dicha constancia ingresando a la página de Internet del Registro General de Adquisiciones del Estado -RGAE- www.rgae.gob.gt.

h) Constancia de Inscripción al Registro Tributario Unificado -RTU-, extendida por la Superintendencia de Administración Tributaria -SAT-.

i) El OFERENTE deberá contar con un mínimo de cinco (5) años de experiencia en la venta, implementación y soporte de soluciones iguales o similares en Guatemala y/o la región de Latinoamérica. Para cumplir con este requerimiento deberá presentar por lo menos 3 cartas de referencia que comprueben el tiempo que se está requiriendo.

   Asimismo, podrá presentar adicionalmente otras cartas de referencia que demuestren el tiempo de experiencia requerido

   * Si el OFERENTE presenta 03 cartas de referencia, no tendrán ponderación siendo estas obligatorias.

j) Listado del personal nacional o extranjero que realizará la implementación, configuración y puesta en funcionamiento del EQUIPO, de acuerdo al ANEXO 6.4 de los presentes DOCUMENTOS DE LICITACIÓN; para su verificación deberá adjuntar los currículums y las certificaciones vigentes que avalen el conocimiento necesario de cada persona, para el efecto deberá presentar lo siguiente:

j.1) Fotocopia legible legalizada de cada uno de los certificados, y/o diplomas u otros documentos consignados en el apartado de: "CERTIFICACIONES RECIBIDAS", por personal propuesto, en donde conste el conocimiento en implementación, configuración y puesta en funcionamiento del OBJETO con características iguales, similares o superiores al OBJETO.

j.2) En el caso de ser profesional deberá acompañar, en original o fotocopia legible legalizada, constancia vigente de ser colegiado activo, la cual se deberá mantener en ese estatus durante la vigencia del CONTRATO, así como renovarla anualmente, tomando en cuenta que los Colegios Profesionales lo extienden únicamente para un (1) año como máximo (Artículo 1 de la Ley de Colegiación Profesional Obligatoria, Decreto Número 72-2001 del Congreso de la República de Guatemala).

j.3) En caso de ser profesional extranjero, estos deberán acompañar, en original o fotocopia legible legalizada, del diploma o título de la institución que lo acredite.

k) Cuadro de ESPECIFICACIONES TÉCNICAS requeridas del EQUIPO, según ANEXO 6.3 de los DOCUMENTOS DE LICITACIÓN, impreso y grabado en formato de texto en un disco compacto, USB o código QR.

l) Catálogos, guías de administración, manuales, documentación y/o guías técnicas, que evidencien el cumplimiento de cada una de las ESPECIFICACIONES TÉCNICAS requeridas.

m) Original de la Certificación Bancaria que acredite la titularidad de las cuentas y operaciones bancarias que posee. Para el efecto deberá contener la información siguiente:

1. Identificación del cuentahabiente.
2. Tipo de cuentas que posee en la entidad bancaria.
3. Promedio de cifras antes del punto decimal de los saldos que posee.
4. Tiempo de manejo de la cuenta.
5. Clase de cuentahabientes.
6. Determinación si posee créditos.
7. Saldo del deudor.
8. Clasificación o categoría del deudor de conformidad con la normativa correspondiente.

El Ministerio de Finanzas Públicas a través de la Dirección General de Adquisiciones del Estado -DGAE- emitirá el formato respectivo que contenga la información detallada.

Dicha certificación deberá ser emitida en un plazo no mayor de dos (2) meses anteriores a la fecha de la recepción de OFERTAS y apertura de PLICAS de la presente LICITACIÓN.

n) Carta del OFERENTE que indique que se compromete a cumplir con lo establecido en el subnumeral 2.30 de los presentes DOCUMENTOS DE LICITACIÓN.

Dentro del tiempo de entrega, el CONTRATISTA deberá considerar la instalación, implementación y pruebas de funcionamiento con el objetivo que la UNIDAD SOLICITANTE reciba el OBJETO instalado, funcional y en condiciones de uso por parte del personal.

o) Original de la Constancia de la Visita realizada a la UNIDAD SOLICITANTE, de acuerdo al ANEXO 6.5.

p) Formulario de identificación del OFERENTE, de acuerdo a los datos solicitados en ANEXO 6.2 de los presentes DOCUMENTOS DE LICITACIÓN.

q) Original o fotocopia legible legalizada de carta que demuestre que es proveedor con el máximo nivel de certificación autorizado por parte del fabricante del EQUIPO ofertado a nivel local como regional.

r) Fotocopia legible legalizada de los siguientes Certificados vigentes:
-ISO 27001:2005 en sistemas de Seguridad de la información
-ISO 9001:2008
-ISO 22301-2012

s) El OFERENTE deberá presentar descripción y certificaciones del Project Manager, especialistas y técnicos establecidos en las especificaciones técnicas.

t) El OFERENTE deberá presentar la matriz de escalamiento según nivel de servicios establecidos en las ESPECIFICACIONES TÉCNICAS.

u) El OFERENTE deberá presentar fotocopia simple del cuadrante de Gartner vigente en donde aparezca la marca ofertada.

v) Si el OFERENTE es Persona Jurídica, deberá presentar Certificación o Constancia de Accionistas, Directivos o Socios que enumere e identifique a los Accionistas, Directivos o Socios que conforman la entidad según corresponda, misma que podrá ser emitida por el Secretario de Actas, algún Miembro del Consejo de Administración o por Perito Contador autorizado por la Superintendencia de Administración Tributaria -SAT-.

En su defecto, podrá presentarse fotocopia legible legalizada del Libro de Accionistas, en la cual se enumere e identifique a los Accionistas que conforman la entidad, indicando el detalle de las acciones que posee cada uno.

La fecha de dichos documentos no deberá exceder de quince (15) días calendario anteriores a la fecha de presentación de la OFERTA. (Artículo 71 del Decreto Número 55-2010 del Congreso de la República de Guatemala, Ley de Extinción de Dominio).

w) Solvencia o cualquier otro documento vigente que para el efecto emita la Inspección General de Trabajo del Ministerio de Trabajo y Previsión Social en donde conste que el OFERENTE, no tiene pendiente el pago de sanciones administrativas y la corrección del

incumplimiento de obligaciones relativas a condiciones generales mínimas de empleo, trabajo, seguridad y salud ocupacional previstas en la legislación de trabajo y previsión social. (Artículo 272 del Decreto Número 1441 del Congreso de la República de Guatemala, Código de Trabajo).

x) El OFERENTE deberá presentar carta en original o fotocopia legible legalizada por medio de la cual certifique que posee la infraestructura necesaria local y/o regional para cubrir requerimientos de garantía de los equipos que forman parte de la solución. Entre ellos e indispensables:

- NOC 24x7x365 a disponibilidad por la duración del proyecto.
- CSOC 24x7x365 a disponibilidad por la duración del proyecto.

2.9 REQUISITOS FUNDAMENTALES

Se consideran Requisitos Fundamentales los siguientes:

a) La presentación del FORMULARIO ELECTRÓNICO en forma física dentro de la PLICA, como se describe en la literal a) del subnumeral 2.8 de los presentes DOCUMENTOS DE LICITACIÓN, su no inclusión y la no coincidencia del código de autenticidad consignado en el FORMULARIO ELECTRÓNICO publicado en GUATECOMPRAS con el presentado físicamente, dará lugar a que la JUNTA, rechace la OFERTA sin responsabilidad alguna de su parte. (Artículos 24 Bis y 30 de la LEY).

La JUNTA no podrá solicitar aclaraciones al apartado “Detalle de la Oferta Económica” contenida en el FORMULARIO ELECTRÓNICO presentado. (Artículo 27 de la LEY).

No será motivo de rechazo por parte de la JUNTA las incongruencias y/o falta de datos que puedan presentarse en los apartados “Datos de los Productos” y “Requisitos solicitados en las bases del proceso” contenidos en el FORMULARIO ELECTRÓNICO, datos que podrán ser subsanados de forma física en virtud que GUATECOMPRAS no permite modificaciones a los datos ingresados en el FORMULARIO ELECTRÓNICO.

b) El Seguro de Caución de Sostenimiento de Oferta como se describe en la literal b) del subnumeral 2.8 de los presentes DOCUMENTOS DE LICITACIÓN, su no inclusión o la presentación del mismo sin la totalidad de la información y/o formalidades requeridas, dará lugar a que la JUNTA, rechace la OFERTA sin responsabilidad alguna de su parte. (Artículo 30 de la LEY).

El Artículo 2 del Acuerdo Ministerial Número 24-2010 del Ministerio de Finanzas Públicas, Normas de Transparencia en los Procedimientos de Compra o Contratación Pública, establece lo siguiente:

En cualquier fase del procedimiento de contratación pública en la que el funcionario o empleado público responsable tenga duda razonable de la veracidad de los documentos o declaraciones presentadas por el OFERENTE o adjudicatario, deberá requerir a éste por escrito, la información y constancias que permitan disipar la duda en un plazo que no exceda de dos (2) días hábiles de conocido el hecho, la cual deberá anexarse al expediente respectivo. Para el efecto, la autoridad concederá al OFERENTE o adjudicatario, audiencia por dos (2) días hábiles y resolverá dentro de un plazo similar.

En caso el OFERENTE o adjudicatario no proporcione la información y constancias requeridas o persista la duda, el funcionario o empleado público responsable de la etapa en que se encuentre el proceso de compra o contratación, resolverá:

a) Rechazar la OFERTA, ó

b) Improbar lo actuado.

En los casos arriba señalados se deberá denunciar el hecho ante el Ministerio Público, sin perjuicio de las demás responsabilidades administrativas o sanciones que le fueran aplicables, debiendo ser inhabilitado en el Sistema GUATECOMPRAS para ser proveedor del Estado, cuando proceda, bajo la responsabilidad de la AUTORIDAD SUPERIOR.

2.10 REQUISITOS NO FUNDAMENTALES

Los demás requisitos que se solicitan en el subnumeral 2.8, se consideran Requisitos No Fundamentales los cuales podrán ser subsanados de forma física en virtud que GUATECOMPRAS no permite modificaciones a los datos ingresados en el FORMULARIO ELECTRÓNICO, la JUNTA podrá solicitar las aclaraciones pertinentes; sin embargo, de no cumplir con la presentación de los mismos físicamente en el plazo indicado por la JUNTA o si fueron presentados sin la totalidad de información y/o formalidades requeridas, la JUNTA rechazará la OFERTA sin responsabilidad de su parte. (Artículos 27 y 30 de la LEY).

2.10.1 DOCUMENTOS RESPALDADOS POR MEDIO DE SISTEMAS INFORMÁTICOS

La impresión de documentos respaldados por medio de los sistemas informáticos de las entidades del Estado, se consideran originales, siempre y cuando, posean firma electrónica, firma electrónica avanzada o cualquier otro medio de certificación electrónica, avalado por el Decreto número 47-2008 del Congreso de la República de Guatemala, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, así como otros documentos que, por disposición especial de otras leyes, puedan ser emitidos de forma electrónica. (Artículo 18 último párrafo del REGLAMENTO).

2.11 DOCUMENTOS NOTARIALES

Las Actas Notariales y las Actas de Legalización de documentos, deberán cumplir con los requisitos establecidos en el Decreto Número 314 del Congreso de la República de Guatemala, Código de Notariado.

2.12 DOCUMENTOS PROVENIENTES DEL EXTRANJERO

Cuando se trate de documentos provenientes del extranjero debe cumplirse con lo establecido en el Decreto Número 1-2016 del Congreso de la República de Guatemala o los Artículos 37 y 38 del Decreto Número 2-89 del Congreso de la República de Guatemala, Ley del Organismo Judicial, según corresponda.

Debiendo presentarse de la manera siguiente:

a) Apostilla o pases legales, según corresponda.

b) Documento(s) proveniente(s) del país de origen en el orden que fueron consignados en la traducción jurada al español (cuando aplique).

2.13 PERFIL DE LOS MIEMBROS TITULARES Y SUPLENTES QUE INTEGRARÁN LA JUNTA, MECANISMO Y ORDEN DE SUSTITUCIÓN

De conformidad con lo establecido en los Artículos 10 y 11 de la LEY, 10 y 12 del REGLAMENTO y la normativa vigente del INSTITUTO; la integración de la JUNTA, deberá tener el perfil siguiente:

La JUNTA estará integrada con los siguientes **titulares:**

a) Un profesional con conocimientos en el negocio a adjudicar, pudiendo ser:

ÁREA	GRADO ACADÉMICO
Profesional	Ingeniería en Informática y Administración Educativa
	Ingeniería en Sistemas de Información y Ciencias de la Computación
	Ingeniería en Sistemas, Informática y Ciencias de la Computación
	Ingeniería en Informática y Sistemas
	Ingeniería en Sistemas
	Ingeniería en Telecomunicaciones
	Ingeniería en Ciencias y Sistemas
	Ingeniería en Electrónica, Informática y Ciencias de la Computación
	Licenciatura en Administración de Sistemas de Información
	Licenciatura en Ciencias de la Computación y Administración de Empresas
	Licenciatura en Informática y Telecomunicaciones
	Licenciatura en Tecnología y Administración de Empresas
	Licenciatura en Tecnología y Administración de las Telecomunicaciones

b) Un trabajador con conocimientos legales, y
c) Un trabajador con conocimientos financieros

Asimismo, se nombrarán dos miembros suplentes que deberán contar con el mismo perfil y conocimientos que el profesional con conocimientos en el negocio a adjudicar y del trabajador con conocimientos legales. Los miembros que funjan como titulares son los únicos que actuarán con voz y voto en la toma de decisiones.

Cuando alguno de los miembros titulares en cualquier parte del proceso deba presentar excusa para ausentarse temporal o definitivamente de sus funciones como miembro de JUNTA, el titular está obligado a informarlo de forma inmediata a la autoridad nominadora, quien deberá resolver lo pertinente. En estos casos, la responsabilidad del miembro titular finaliza al momento en que le sea notificada la aceptación de la excusa por parte de la autoridad nominadora. Esta disposición será aplicable de igual manera a los miembros suplentes que presenten excusas.

La ausencia injustificada de alguno de los miembros titulares en cualquier parte del proceso de contratación no suspende su continuidad, debiendo los miembros suplentes asumir la titularidad de forma inmediata para cubrir la ausencia. Los miembros titulares o suplentes de JUNTA, que incumplan con sus funciones o que se ausenten injustificadamente del lugar

donde deben estar constituidos, serán sancionados conforme al régimen sancionatorio administrativo del Estado o del INSTITUTO, según sea el caso, sin perjuicio de que se deduzcan las demás responsabilidades civiles y penales que se puedan derivar del hecho.

En caso de ausencia de uno o dos miembros de la JUNTA el día programado para la presentación, recepción de OFERTAS y apertura de PLICAS, anteponiendo los intereses del INSTITUTO, dicho acto público no se suspenderá, siempre que se encuentren presentes por lo menos tres (3) miembros de la JUNTA, quienes indistintamente de su nombramiento, actuarán en calidad de miembros titulares. Con relación a esta disposición, los miembros presentes no podrán justificar falta de idoneidad, para evitar la continuidad del proceso. La JUNTA será quien dirija el referido acto público y deberá dejar constancia de todo lo actuado en el acta correspondiente.

En caso de ausencia de alguno de los miembros titulares estos serán sustituidos de forma inmediata de acuerdo al mecanismo siguiente:

1. En caso de excusarse o ausentarse el titular con conocimientos en el negocio a adjudicar, éste será sustituido inmediatamente por el suplente con el mismo perfil profesional.

2. En caso de excusarse o ausentarse el titular con conocimientos legales o financieros, este será sustituido inmediatamente por el suplente con conocimientos legales.

La JUNTA podrá solicitar, según corresponda, asesoría en la materia específica o solicitar asistencia de asesores de otras entidades del sector público.

En caso de aceptación por parte de la Autoridad nominadora de la excusa de un titular o suplente por ausencia temporal o definitiva, ésta emitirá el nombramiento del suplente como titular y nombrará nuevo suplente, dentro del plazo establecido en la LEY, posterior a conocerse el hecho que genera la suplencia, con el fin que la JUNTA siempre se encuentre integrada con el número de miembros correspondientes.

2.14 PRESENTACIÓN Y RECEPCIÓN DE OFERTAS

Las OFERTAS deberán ser presentadas ante la JUNTA en el lugar, dirección, fecha y hora establecidos en el cronograma de actividades de los presentes DOCUMENTOS DE LICITACIÓN. (Artículos 24 de la LEY y 20 del REGLAMENTO). La JUNTA extenderá una constancia de la recepción de la OFERTA.

2.14.1 AUSENCIA DE OFERTAS

En caso que no se reciban OFERTAS la JUNTA elevará el expediente a la AUTORIDAD ADMINISTRATIVA SUPERIOR, a efecto que prorrogue el plazo de presentación y recepción de OFERTAS. (Artículo 32 de la LEY).

2.14.2 SEGUNDA AUSENCIA DE OFERTAS

En caso no se reciban OFERTAS la Autoridad Competente podrá autorizar que el proceso se lleve a cabo a través de Adquisición Directa por Ausencia de Ofertas, con los mismos requisitos y condiciones establecidas en el presente proceso, debiendo registrarse en el sistema GUATECOMPRAS el estatus de desierto, de conformidad con la legislación vigente y la normativa interna aplicable. (Artículo 32 de la LEY).

2.15 APERTURA DE PLICAS

Al finalizar el período de presentación y recepción de OFERTAS, en acto público la JUNTA procederá a la apertura de PLICAS en el orden que fueron recibidas, dando lectura en voz alta a los nombres de los OFERENTES y el Precio Total y/o Monto Ofertado de cada OFERTA.

De lo actuado se faccionará Acta de Recepción de Ofertas y Apertura de Plicas, suscrita por los miembros de la JUNTA, la cual, con el listado de OFERENTES, se publicará en GUATECOMPRAS. (Artículos 24 de la LEY y 20 del REGLAMENTO).

2.16 ACLARACIONES

La JUNTA podrá solicitar, a cualquier OFERENTE, las aclaraciones que considere pertinentes, siempre y cuando se refieran a requisitos y condiciones relacionados con el OBJETO, que hayan sido solicitados en los presentes DOCUMENTOS DE LICITACIÓN; dichos requisitos no podrán modificar la OFERTA presentada. (Artículo 27 de la LEY).

2.17 MOTIVOS PARA RECHAZAR OFERTAS

Previo a la calificación de las OFERTAS, la JUNTA analizará el cumplimiento de los requisitos exigidos, pudiendo sin responsabilidad de su parte rechazarlas por las causas establecidas en la LEY y el REGLAMENTO, además de las siguientes:

a) Si los Requisitos Fundamentales exigidos en el subnumeral 2.9 de los presentes DOCUMENTOS DE LICITACIÓN, no cumplen con las características solicitadas o si faltare cualquiera de ellos; dará lugar a que la JUNTA, rechace la OFERTA sin responsabilidad de su parte. (Artículos 30 de la LEY).

b) Si la JUNTA concedió plazo común para presentar los Requisitos No Fundamentales contemplados en el subnumeral 2.10 de los presentes DOCUMENTOS DE LICITACIÓN y éstos no fueron presentados dentro de dicho plazo, o si fueron presentados sin la totalidad de la información y/o formalidades requeridas, dará lugar a que la JUNTA, rechace la OFERTA sin responsabilidad de su parte. (Artículos 30 de la LEY).

c) Si no cumple a satisfacción con las ESPECIFICACIONES GENERALES, ESPECIFICACIONES TÉCNICAS y DISPOSICIONES ESPECIALES solicitadas para el OBJETO de la presente Licitación.

d) Si el Precio Unitario o el Monto Ofertado no se ajusta a las condiciones establecidas en la literal b) del subnumeral 2.7.1 de los presentes DOCUMENTOS DE LICITACIÓN.

e) Si el tiempo de entrega ofertado es mayor de ciento ochenta (180) días calendario.

f) Si los documentos presentados modifican o tergiversan lo estipulado por estos DOCUMENTOS DE LICITACIÓN.

g) Si el Monto Ofertado, calidades u otras condiciones ofrecidas, son inconvenientes a los intereses del INSTITUTO. (Artículos 30 de la LEY).

h) Si a juicio de la JUNTA, existen indicios de pacto colusorio. En este caso están obligados a realizar la denuncia a las autoridades correspondientes. (Artículos 25 y 25 Bis de la LEY).

i) Si se dan los supuestos establecidos en el Artículo 2 del Acuerdo Ministerial Número 24-2010 del Ministerio de Finanzas Públicas, Normas de Transparencia en los Procedimientos de Compra o Contratación Pública.

2.18 METODOLOGÍA DE CALIFICACIÓN

Las OFERTAS recibidas serán calificadas por la JUNTA de acuerdo a la LEY, el REGLAMENTO y a la siguiente metodología, para determinar si las mismas cumplen con los requisitos solicitados en los presentes DOCUMENTOS DE LICITACIÓN.

La metodología a utilizar por la JUNTA se dará en tres fases: **1.** Verificación del cumplimiento de los Requisitos Fundamentales por parte del OFERENTE, **2.** Verificación del cumplimiento de los Requisitos No Fundamentales por parte del OFERENTE, **3.** Calificación de las OFERTAS conforme a los Criterios de calificación establecidos en los presentes DOCUMENTOS DE LICITACIÓN.

La JUNTA deberá verificar la información ingresada electrónicamente en GUATECOMPRAS con la documentación presentada en la PLICA. La JUNTA podrá solicitar aclaraciones a cualquier OFERENTE, sin que la OFERTA sea modificada. (Artículos 27 de la LEY y 19 del REGLAMENTO).

2.18.1 VERIFICACIÓN DE LOS REQUISITOS FUNDAMENTALES

La JUNTA verificará el cumplimiento de los Requisitos Fundamentales, si el OFERENTE los cumple, pasará a determinar el cumplimiento de dichos requisitos en otra OFERTA y así sucesivamente hasta agotar todas las revisiones.

Si el OFERENTE no cumple con la entrega de algún Requisito Fundamental, se anotará en el Acta correspondiente, el nombre del OFERENTE y el o los Requisitos Fundamentales no cumplidos, o la presentación de los mismos sin la totalidad de la información y/o formalidades requeridas, dará lugar a rechazar la OFERTA, tal como se estipula en el subnumeral 2.17 literal a) de los presentes DOCUMENTOS DE LICITACIÓN.

La JUNTA, deberá utilizar el precio de mercado en condiciones de competencia que se determine.

2.18.2 VERIFICACIÓN DE LOS REQUISITOS NO FUNDAMENTALES

De las OFERTAS que hubieren cumplido con los Requisitos Fundamentales, la JUNTA procederá a la revisión del cumplimiento de los Requisitos No Fundamentales, verificando la información consignada en GUATECOMPRAS con la documentación presentada en la PLICA, validando que hayan cumplido con todos y cada uno de los requisitos solicitados.

Si algún OFERENTE no cumplió con la entrega de Requisitos No Fundamentales o la presentación de los mismos sin la totalidad de la información y/o formalidades requeridas, la JUNTA elaborará oficio de “Solicitud de aclaración y/o documentación complementaria”, el que debe ser cumplido en el plazo que la JUNTA determine. La solicitud efectuada debe ser publicada en GUATECOMPRAS y la JUNTA verificará el cumplimiento de lo solicitado.

El INSTITUTO, a través de la Dependencia correspondiente, realizará las acciones pertinentes para obtener un análisis de mercado, el cual establecerá un precio de mercado en condiciones de competencia tomando en consideración las ESPECIFICACIONES

GENERALES, ESPECIFICACIONES TÉCNICAS Y DISPOSICIONES ESPECIALES requeridas para el presente evento.

Si la JUNTA determina que ningún OFERENTE cumple con todos los requisitos, deberá sustentar y detallar tal extremo en el Acta correspondiente.

2.18.3 CALIFICACIÓN DE LA OFERTA

La JUNTA calificará únicamente las OFERTAS que cumplan con los Requisitos Fundamentales, Requisitos No Fundamentales, y cumplimiento de ESPECIFICACIONES GENERALES, ESPECIFICACIONES TÉCNICAS y DISPOSICIONES ESPECIALES y que no hayan sido rechazadas por las circunstancias que se establecen en el subnumeral 2.17 de los presentes DOCUMENTOS DE LICITACIÓN.

Las OFERTAS que hayan cumplido con todos y cada uno de los requisitos solicitados podrán continuar con la etapa de Calificación de OFERTA.

2.18.3.1 CRITERIOS DE CALIFICACIÓN Y SU PONDERACIÓN

La JUNTA, para determinar cuál es la oferta más conveniente y favorable para los intereses del INSTITUTO, utilizará los criterios que se describen a continuación:

Criterios de Calificación (Artículos 28 de la LEY y 19 de su REGLAMENTO):

DESCRIPCIÓN	Punteo a asignar
TIEMPO DE ENTREGA	25 Puntos
EXPERIENCIA	25 Puntos
MONTO OFERTADO	50 Puntos
TOTAL	**100 Puntos**

a) TIEMPO DE ENTREGA……25 puntos

La JUNTA evaluará con veinticinco (25) puntos al OFERENTE que ofrezca entregar lo requerido en el menor tiempo (en días calendario); éste no podrá ser mayor de ciento ochenta (180) días calendario, contados a partir de la notificación de la resolución de aprobación del CONTRATO y se calificará de la siguiente manera:

$$Calificación\ tiempo\ de\ entrega\ = \left(\frac{T_m}{T_N}\right) \times 25$$

T_m = Menor tiempo de entrega ofertado
T_N = Tiempo de entrega ofertado por el Oferente N (Cada tiempo de entrega subsiguiente al de menor tiempo de entrega).

Dentro del tiempo de entrega, el CONTRATISTA deberá considerar la instalación, implementación y pruebas de funcionamiento con el objetivo que la UNIDAD SOLICITANTE reciba el OBJETO instalado, funcional y en condiciones de uso por parte del personal.

b) EXPERIENCIA……25 puntos

Para calificar la experiencia, la JUNTA tomará en cuenta los documentos solicitados en la subliteral i), del subnumeral 2.8 de los Documentos de LICITACIÓN, de la manera siguiente:

Si presenta cuatro (4) cartas de referencia	10 puntos
Si presenta de cinco (5) a siete (7) cartas de referencia	15 puntos
Si presenta ocho (8) cartas de referencia en adelante	25 puntos

* Se ponderarán únicamente las cartas de referencia, presentadas por el OFERENTE, adicionales a las solicitadas en la literal i) del subnumeral 2.8 que demuestren el tiempo de experiencia requerido.

* Si el OFERENTE presenta 03 cartas de referencia que demuestren la experiencia requerida en la literal i) del subnumeral 2.8 no tendrá ponderación alguna, ya que estas son obligatorias.

c) MONTO OFERTADO……...50 puntos

La JUNTA calificará con cincuenta (50) puntos la OFERTA económica del OFERENTE que presente el Monto Ofertado más bajo, con relación al resto de los OFERENTES a quien se les calificará con los puntos que en forma inversamente proporcional les corresponda con respecto al total de los puntos de la OFERTA más favorable.

Para la calificación la JUNTA tomará en cuenta la fórmula siguiente:

$$Calificación\ monto\ ofertado = \left(\frac{P_m}{P_N}\right) \times 50$$

P_m = Menor precio ofertado
P_N = Precio ofertado

CUADRO DE CALIFICACIÓN DE OFERTA

OFERENTE	Tiempo de entrega (25 puntos)	Experiencia (25 puntos)	Monto Ofertado (50 puntos)	Total (100 puntos)
Oferente 1				
Oferente 2				

7ª. Avenida 22-72, zona 1, Centro Cívico Guatemala, C. A. PBX: 2412-1224, ext. 1238

2.19 ADJUDICACIÓN

Dentro del plazo indicado en el cronograma de actividades de los presentes DOCUMENTOS DE LICITACIÓN, o la prórroga autorizada si la hubiere, la JUNTA adjudicará el OBJETO de la presente Licitación al OFERENTE que cumpla con lo requerido en los presentes DOCUMENTOS DE LICITACIÓN y presente la OFERTA que obtenga el mayor punteo de la suma de las ponderaciones asignadas en los criterios de calificación indicados anteriormente. (Artículo 33 de la LEY y 21 del REGLAMENTO).

En caso que dos (2) o más OFERENTES se encuentren en igualdad de condiciones con respecto a la puntuación obtenida, la JUNTA podrá adjudicar al OFERENTE que posea el monto ofertado más bajo, en caso de continuar con la igualdad, podrá adjudicar al OFERENTE que posea mayor cantidad de años de experiencia en la venta, instalación y configuración de soluciones iguales o similares dentro del territorio de Guatemala.

En el Acta de Adjudicación de Ofertas se dejará constancia de lo siguiente:

a) OFERTAS rechazadas y su razón (si fuera el caso).

b) Cuadros o detalles de la evaluación efectuada a cada una de las OFERTAS que no fueron rechazadas, conteniendo el criterio de evaluación y el puntaje obtenido por cada OFERTA. (Artículo 21 del REGLAMENTO).

c) Identificación del OFERENTE y OBJETO adjudicado.

d) El tiempo de entrega ofertado por el adjudicado.

e) Calificación de los OFERENTES que clasifiquen sucesivamente, para que en caso el adjudicatario no suscribiere el CONTRATO respectivo, la negociación pueda llevarse a cabo con solo el subsiguiente clasificado en su orden. (Artículos 33 de la LEY).

La notificación del Acta de Adjudicación de Ofertas, conteniendo el cuadro de calificación de OFERTAS, se efectuará por vía electrónica a través de GUATECOMPRAS dentro de los dos (2) días hábiles siguientes a la fecha de la emisión. (Artículos 33 y 35 de la LEY y 21 del REGLAMENTO).

2.20 APROBACIÓN DE LO ACTUADO POR LA JUNTA

Publicada en GUATECOMPRAS la adjudicación y contestadas las inconformidades, si las hubiere, la JUNTA remitirá el expediente a la AUTORIDAD SUPERIOR, dentro de los dos (2) días hábiles siguientes. La AUTORIDAD SUPERIOR aprobará o improbará lo actuado por la JUNTA, con causa justificada, de conformidad con lo establecido en la LEY, dentro de los cinco (5) días de recibido el expediente. La AUTORIDAD SUPERIOR dejará constancia escrita de lo actuado.

Si la AUTORIDAD SUPERIOR imprueba lo actuado por la JUNTA, deberá devolver el expediente para su revisión, dentro del plazo de dos (2) días hábiles posteriores de adoptada la decisión. La JUNTA, con base en las observaciones formuladas por la AUTORIDAD SUPERIOR, podrá confirmar o modificar su decisión original, en forma razonada, dentro del plazo de cinco (5) días hábiles de recibido el expediente, revisará lo actuado y hará la adjudicación conforme a la LEY y los DOCUMENTOS DE LICITACIÓN.

Dentro de los dos (2) días hábiles posteriores a la decisión, la JUNTA devolverá el expediente a la AUTORIDAD SUPERIOR, quien dentro de los cinco (5) días hábiles subsiguientes podrá aprobar, improbar o prescindir de la negociación.

En caso de improbar, se notificará electrónicamente a través de GUATECOMPRAS, dentro de los dos (2) días hábiles siguientes, dando por concluido el evento. En caso de prescindir, aplicará lo establecido en el Artículo 37 de la LEY. En los casos en los que la AUTORIDAD SUPERIOR decida improbar o prescindir, razonará la decisión en la resolución correspondiente. (Artículos 36 de la LEY y 23 del REGLAMENTO).

2.21 SUSCRIPCIÓN Y APROBACIÓN DEL CONTRATO

El CONTRATO detallará todas las condiciones que regirán el OBJETO de la presente negociación y se elaborará con base a la LEY y su REGLAMENTO, a la OFERTA adjudicada, a las ESPECIFICACIONES GENERALES, ESPECIFICACIONES TÉCNICAS**,** DISPOSICIONES ESPECIALES y ANEXOS de estos DOCUMENTOS DE LICITACIÓN. La suscripción y aprobación del mismo se realizará dentro del plazo y formalidades establecidos en la LEY. (Artículos 47 y 48 de la LEY y 42 del REGLAMENTO).

El CONTRATO debe incluir la cláusula especial siguiente: “CLÁUSULA RELATIVA AL COHECHO: Yo el Contratista, manifiesto que conozco las penas relativas al delito de cohecho así como las disposiciones contenidas en el Capítulo III del Título XIII del Decreto 17-73 del Congreso de la República, Código Penal. Adicionalmente, conozco, las normas jurídicas que facultan a la Autoridad Superior de la entidad afectada para aplicar las sanciones administrativas que pudieren corresponderme, incluyendo la inhabilitación en el Sistema GUATECOMPRAS.” (Artículo 3 del Acuerdo Ministerial Número 24-2010 del Ministerio de Finanzas Públicas, Normas de Transparencia en los Procedimientos de Compra o Contratación Pública).

Recibido el expediente que contiene la aprobación del CONTRATO por la Autoridad competente, el DEPARTAMENTO DE ABASTECIMIENTOS, deberá publicar en GUATECOMPRAS el CONTRATO con su respectiva aprobación y notificar electrónicamente dicho CONTRATO, al Registro de Contratos de la Contraloría General de Cuentas, Unidad de Digitalización y Resguardo de Contratos. (Acuerdo Número A-038-2016 de la Contraloría General de Cuentas); asimismo, se procederá a notificar a la UNIDAD SOLICITANTE del INSTITUTO.

Notificado lo anterior, se debe publicar en GUATECOMPRAS, la Constancia de Recepción de Contrato que para el efecto emita la Contraloría General de Cuentas, como máximo al día hábil siguiente.

2.22 NOTIFICACIONES

Las notificaciones que surjan del presente proceso serán efectuadas por vía electrónica a través de GUATECOMPRAS y deberán hacerse en el plazo que establece la LEY, REGLAMENTO y demás normativa vigente, y surtirán sus efectos al día siguiente de su publicación en dicho sistema. (Artículo 35 de la LEY).

2.23 GARANTÍAS

Los seguros deberán publicarse en GUATECOMPRAS y para efectos de lo regulado en el Artículo 69 de la LEY se procederá de la manera siguiente:

a) Las JUNTAS a las que se refiere el Artículo 10 de la LEY, serán responsables de verificar la autenticidad del Seguro de Caución de Sostenimiento de Oferta, descrito en el subnumeral 2.23.1, mediante la certificación requerida en la literal c) del subnumeral 2.8 de los presentes DOCUMENTOS DE LICITACIÓN.

b) Las autoridades suscriptoras de los contratos serán responsables de verificar la autenticidad del seguro descrito en los subnumerales 2.23.2 y 2.23.3, mediante la certificación de autenticidad que emita la aseguradora, misma que deberá anexarse a la póliza respectiva, en donde se hará constar que ha sido emitida en cumplimiento al Decreto Número 25-2010 del Congreso de la República de Guatemala, Ley de la Actividad Aseguradora y que el firmante de la póliza posee las facultades y competencias respectivas.

2.23.1 SEGURO DE CAUCIÓN DE SOSTENIMIENTO DE OFERTA

Formalizado mediante póliza, extendida por una institución afianzadora debidamente autorizada para operar en la República de Guatemala. (Artículos 64 y 69 de la LEY, 53 y 59 del REGLAMENTO; Artículos 3 literal b), 106 y 109, Decreto Número 25-2010 del Congreso de la República de Guatemala, Ley de la Actividad Aseguradora).
Deben tomarse en cuenta las consideraciones siguientes:

a) Extendida a favor del INSTITUTO.

b) Debe garantizar a:
- Si es persona individual a nombre del Propietario de la Empresa.
- Si es persona jurídica a nombre de la razón social o denominación social.

c) Con vigencia de ciento veinte (120) días a partir de la fecha de recepción y apertura de PLICAS. Sin embargo, con el adjudicatario, puede convenirse su prórroga.

d) Constituida por un porcentaje no menor del uno por ciento (1%) ni mayor del cinco por ciento (5%) del valor total del CONTRATO.

e) Se hará efectivo en cualquiera de los casos siguientes:

1. Si el adjudicatario no sostiene su OFERTA.

2. Si no concurre a suscribir el CONTRATO respectivo dentro del plazo legal correspondiente o si habiéndolo hecho no presenta el Seguro de Caución de Cumplimiento dentro del plazo de quince (15) días siguientes a la firma del CONTRATO. (Artículos 47 de la LEY y 53 del REGLAMENTO).

2.23.2 SEGURO DE CAUCIÓN DE CUMPLIMIENTO

Dentro del plazo de quince (15) días siguientes a la suscripción del CONTRATO, el CONTRATISTA deberá presentar Seguro de Caución de Cumplimiento de Contrato. (Artículos 65 y 69 de la LEY; Artículos 53, 55 y 56 del REGLAMENTO; Artículos 3 literal b), 106 y 109 del Decreto Número 25-2010 del Congreso de la República de Guatemala, Ley de la Actividad Aseguradora).

Deberá tomarse en cuenta las consideraciones siguientes:

a) Formalizado mediante póliza extendida a favor del INSTITUTO, por una institución afianzadora debidamente autorizada para operar en la República de Guatemala.

b) Constituida por una suma equivalente al diez por ciento (10%) del monto del CONTRATO.

c) El CONTRATISTA se compromete a mantener vigente el Seguro de Caución de Cumplimiento hasta que el INSTITUTO a través de la UNIDAD SOLICITANTE, extienda la constancia de haber recibido a satisfacción la totalidad de lo contratado en la presente negociación.

d) El Seguro de Caución de Cumplimiento se hará efectivo si el CONTRATISTA incumple con alguna de las condiciones establecidas en los presentes DOCUMENTOS DE LICITACIÓN, en el CONTRATO, o si el OBJETO entregado no fuese el adjudicado.

e) El seguro debe garantizar exacta y fielmente las obligaciones a cargo del CONTRATISTA.

2.23.3 SEGURO DE CAUCIÓN DE CALIDAD Y/O FUNCIONAMIENTO

El CONTRATISTA, deberá otorgar Seguro de Caución de Calidad y/o Funcionamiento, por el equivalente al quince por ciento (15%) del valor original del CONTRATO, como requisito previo para la entrega del OBJETO, la cual tendrá una vigencia de tres (3) años en sitio, contados a partir de la fecha de recepción del OBJETO. (Artículos 67 y 69 de la LEY).

2.24 PLAZO CONTRACTUAL

Periodo que dispone el CONTRATISTA para el cumplimiento del OBJETO del CONTRATO, el cual será de cuarenta y cinco (45) meses y empezará a contar a partir del día siguiente de la notificación de la Resolución de aprobación del CONTRATO. (Artículo 2 numeral 20) del REGLAMENTO).

2.25 VIGENCIA DEL CONTRATO

La vigencia del CONTRATO será a partir del día siguiente de la notificación de la Resolución de aprobación del CONTRATO, hasta que el INSTITUTO a través de la UNIDAD SOLICITANTE extienda la constancia de haber recibido a satisfacción la totalidad de lo contratado en la presente negociación. (Artículo 56 de la LEY y Artículo 2 numeral 32) del REGLAMENTO).

2.26 RECEPCIÓN

La AUTORIDAD ADMINISTRATIVA SUPERIOR nombrará una Comisión Receptora, la cual estará integrada por tres (3) técnicos con conocimientos en la materia propuestos por la UNIDAD SOLICITANTE, para recibir el OBJETO de la presente negociación, quienes dejarán constancia de lo actuado en Acta, aplicando en lo que fuere procedente lo que establece el Artículo 55 de la LEY.

La Comisión Receptora deberá verificar que el EQUIPO sea entregado bajo la modalidad “LLAVE EN MANO”, garantizando la compatibilidad, integración, interoperabilidad y funcionalidad del OBJETO de este evento.

Asimismo, deberá verificar que el licenciamiento propuesto por el CONTRATISTA corresponda al entregado.

2.27 INHABILITACIÓN EN GUATECOMPRAS

Se inhabilitará en el Registro General de Adquisiciones del Estado, -RGAE- a los OFERENTES o CONTRATISTAS que incurran en cualquiera de las causales que define la LEY y su REGLAMENTO, entre ellas:

2.27.1 Que exista pacto colusorio entre dos o más OFERENTES. (Artículo 25 Bis de la LEY).
2.27.2 Que, de comprobarse pacto colusorio, se procederá a realizar lo descrito en el Artículo 25 Bis de la LEY.
2.27.3 Que no suscriba el CONTRATO dentro del plazo legal. (Artículo 84 de la LEY).
2.27.4 Que incurra en retraso en la entrega. (Artículo 85 de la LEY).
2.27.5 Que incurra en variación de calidad o cantidad del OBJETO del CONTRATO. (Artículo 86 de la LEY).
2.27.6 Que proporcione información falsa.
2.27.7 Que interponga acciones frívolas e impertinentes que entorpezcan el desarrollo normal del proceso de contratación. (Artículo 63 del REGLAMENTO).
2.27.8 Otras que correspondan.

2.28 SANCIONES

El incumplimiento a las condiciones estipuladas en el CONTRATO o en los presentes DOCUMENTOS DE LICITACIÓN, estará sujeto a las sanciones que establece la LEY y su REGLAMENTO.

2.29 RETRASO EN LA ENTREGA

Si el CONTRATISTA incurriere en retraso en la entrega del OBJETO requerido, se le sancionará, de conformidad con lo que establece el Artículo 85 de la LEY y Artículo 62 Bis de su REGLAMENTO.

2.30 LUGAR Y TIEMPO DE ENTREGA

El CONTRATISTA deberá entregar el EQUIPO instalado y funcionando en la UNIDAD SOLICITANTE. El tiempo de entrega será el propuesto por el CONTRATISTA en el FORMULARIO ELECTRÓNICO, el cual no podrá ser mayor a ciento ochenta (180) días calendario contados a partir de la notificación de la resolución de aprobación del CONTRATO.

El medio de transporte a utilizar será el más adecuado que estime el CONTRATISTA, en resguardo del EQUIPO a trasladar desde su sede hasta la UNIDAD SOLICITANTE.

2.31 FACTURA ELECTRÓNICA

El CONTRATISTA para requerir el pago deberá presentar la Factura Electrónica en Línea -FEL-, de conformidad a lo establecido en: Acuerdo de Directorio Número 13-2018 y Resolución Número SAT-DSI-243-2019, ambos de la Superintendencia de Administración Tributaria -SAT-; y Oficio Circular Número 02-2019 de la Dirección General de Adquisiciones del Estado -DGAE-.

2.32 FORMA DE PAGO

El INSTITUTO pagará el OBJETO de la adquisición que fue requerido por la UNIDAD SOLICITANTE recibido y a entera satisfacción, en dos (2) pagos, así: Primer pago de 85% del monto total, luego de la entrega de la Solución Integrada de Ciberseguridad; Segundo pago de 15% al finalizar la configuración, implementación, capacitación y puesta en

funcionamiento de la solución; dentro del plazo de treinta (30) días posteriores a la fecha de presentación de la Factura Electrónica FEL y demás documentación que se le requiera, por medio de depósito en cuenta monetaria del Banco de Desarrollo Rural, Sociedad Anónima, -BANRURAL- u otros del sistema que el CONTRATISTA haya registrado.

El trámite de dicho pago estará a cargo de la UNIDAD SOLICITANTE, quien procederá de conformidad con la normativa del INSTITUTO. En caso que el OBJETO no sea pagado en el ejercicio fiscal vigente, se afectará la partida presupuestaria autorizada para el ejercicio fiscal siguiente, por el órgano director del INSTITUTO y que corresponda a la UNIDAD SOLICITANTE. (Artículo 62 de la LEY).

3. ESPECIFICACIONES GENERALES

La Subgerencia de Tecnología requiere una (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD para el Instituto Guatemalteco de Seguridad Social -IGSS-, de conformidad con las ESPECIFICACIONES TÉCNICAS REQUERIDAS Y DISPOSICIONES ESPECIALES establecidas.

4. ESPECIFICACIONES TÉCNICAS REQUERIDAS:

Se debe proveer una Solución que permita integrar plataformas y herramientas de ciberseguridad en un ecosistema cooperativo que brinde interoperabilidad para proteger los diferentes vectores de ataque existentes de forma coordinada y con posibilidad de escalar de forma modular de acuerdo con lo expresado por la organización Gartner bajo el concepto de "Arquitectura de malla o tejido de seguridad cibernética" o "Cybersecurity Mesh Architecture" en idioma inglés.

4.1

Módulo	Clasificación Funcional		Descripción de la Función
Descripción General de la Solución	Integración y automatización de la Solución	1	Se debe proveer una solución que permita integrar plataformas y herramientas de ciberseguridad en un ecosistema cooperativo que brinde interoperabilidad para proteger los diferentes vectores de ataque existentes de forma coordinada y con posibilidad de escalar de forma modular de acuerdo con lo expresado por la organización Gartner bajo el concepto de "Arquitectura de malla o tejido de seguridad cibernética" o "Cybersecurity Mesh Architecture" en inglés.
		2	La Solución ofertada debe tener capacidades de integración y automatización dentro de las plataformas, herramientas de red y ciberseguridad que la conforman.
		3	La Solución ofertada debe considerar como mínimo la protección de dispositivos (endpoints y servidores), aplicaciones, la red, el centro de datos como mínimo.
		4	La Solución debe contar con herramientas contra amenazas persistentes de acuerdo con lo descrito en las especificaciones técnicas de los elementos necesarios solicitados.
		5	La Solución debe contar con herramientas unificadas de monitoreo capaces de generar reportería y tableros que permitan la visibilidad de las amenazas que sean descubiertos por las herramientas de seguridad que la componen. Las herramientas de monitoreo deberán dar visibilidad del estado de salud de los componentes de la Solución, así como considerar la integración de indicadores de compromiso que puedan ser utilizados por otros elementos de la Solución para identificar amenazas.

		6	La Solución debe contar con un subsistema de identificación y accesos para las personas responsables de gestionar y monitorear los componentes de esta.
		7	No se considerarán las ofertas que propongan una arquitectura con silos o islas de protección que no son capaces de interactuar y automatizar tareas de defensa en conjunto con las otras herramientas propuestas como parte de la arquitectura.
		8	El OFERENTE deberá considerar los servicios profesionales necesarios para realizar las integraciones y automatizaciones que a continuación se describen como mínimo, esto como beneficio de la arquitectura integral requerida.
		Se requiere de las siguientes integraciones	
		1	El equipo de seguridad de red (Firewall) debe integrarse a la plataforma de Sandboxing, como mínimo los firewalls incluidos en la Solución deben ser capaces de enviar archivos sospechosos a la plataforma de Sandboxing y la misma debe ser capaz de analizarlos y realizar pruebas en ambiente aislado a la red y con esto determinar si son maliciosos o no. En caso se confirme que son maliciosos debe retroalimentar a los demás elementos de la Solución para que puedan identificar la amenaza de día cero y bloquear las siguientes descargas del archivo malicioso.
		2	El equipo de balanceo de carga de aplicaciones y el Firewall de Aplicaciones Web (WAF) debe integrarse a la solución de Sandboxing, para evitar el envío de amenazas de día 0 en la carga de archivos a los servidores que estará protegiendo.
		3	Detección y respuesta extendida para amenazas avanzadas en el Endpoint o EDR debe integrarse a la solución de Sandboxing de forma nativa, para evaluar archivos sospechosos e identificar amenazas de día cero en conjunto, al detectar la amenaza debe retroalimentar a los demás componentes de la Solución incluyendo al EDR para que puedan aislar la amenaza y mitigar o de ser posible eliminar el riesgo de forma proactiva.
		4	El Control de Acceso a la Red (NAC) debe ser capaz de recibir alertas de seguridad del Firewall, con la finalidad de automatizar la respuesta y aislar a la computadora a nivel de capa 2, colocándolo en una VLAN de cuarentena.
		5	El SIEM debe poder enviar al Firewall direcciones IP maliciosas identificadas en la red, con la finalidad de automatizar el bloqueo a nivel de Firewall de la amenaza.

		6	Los equipos de seguridad de red (Firewall) debe poder integrarse con la plataforma de NDR por protocolo ICAP para enviar archivos, logrando así que NDR pueda identificar la amenaza y automatizar la respuesta con el Firewall, bloqueando así el malware de manera más efectiva.
		7	El Control de Acceso a la Red "NAC", protección de endpoint, doble factor de autenticación y Firewalls deben poder integrarse tanto con la plataforma de analítica que ya tiene el instituto como con el SIEM que se está solicitando en este evento.

4.2

Módulo	Clasificación Funcional		Descripción de la Función
Dos (2) Dispositivos Next Generation Firewall para seguridad lógica de redes internas y Data Center.	Firewall de protección de redes internas y Data Center.	1	Puerto de administración dedicada, fuera de banda o similar de tipo RJ45
		2	Puerto de consola serial
		3	2 puertos 10 GE / GE RJ45
		4	2 puertos 25GE SFP28/ 10GE SFP+
		5	30 puertos 25GE SFP28/ 10GE SFP+/ GE SFP
		6	6 puertos 100GE QSFP28/ 40GE QSFP+ Slots
		7	Rendimiento de IPS 72 Gbps
		8	Rendimiento de NGFW 65 Gbps
		9	Rendimiento de protección de amenazas 63 Gbps
		10	Rendimiento de inspección SSL 63 Gbps
		11	Latencia de Firewall 4 microsegundos
		12	Rendimiento de Firewall de 630 Mpps
		13	Sesiones concurrentes TCP 140 millones como mínimo
		14	Nuevas sesiones/segundo 1 millón
		15	Políticas de Firewall 200,000 como mínimo
		16	Rendimiento de control de aplicaciones 135 Gbps
		17	El equipo debe ser líder en el cuadrante mágico de Gartner para WAN Edge y Network Firewalls.
		18	Soporte para la creación de dominios virtuales
		19	El equipo debe ser compatible con plataforma de logs y gestión de Firewalls actualmente en el Instituto.
		20	Soporte de alta disponibilidad en modos Activo-Activo, Activo-Pasivo y Clustering
		21	2 unidades de rack con kit de montaje y tornillos incluidos para su instalación
		22	Fuentes de poder intercambiables en caliente (hot-swap) y redundantes 100-240V AC, 50-60Hz

		A. Funcionalidades Generales	
		1	Los equipos deben consistir en una Solución de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.
		2	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
		3	Las funcionalidades de protección de red que conforman la Solución de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;
		4	La Solución debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
		5	Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;
		6	La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
		7	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
		8	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
		9	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
		10	Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);
		11	Los dispositivos de protección de red deben soportar DHCP Relay;
		12	Los dispositivos de protección de red deben soportar DHCP Server;
		13	Los dispositivos de protección de red deben soportar sFlow;
		14	Los dispositivos de protección de red deben soportar Jumbo Frames;
		15	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
		16	Debe ser compatible con NAT dinámica (varios-a-1);
		17	Debe ser compatible con NAT dinámica (muchos-a-muchos);
		18	Debe soportar NAT estática (1-a-1);
		19	Debe admitir NAT estática (muchos-a-muchos);

		20	Debe ser compatible con NAT estático bidireccional 1-a-1;
		21	Debe ser compatible con la traducción de puertos (PAT);
		22	Debe ser compatible con NAT Origen;
		23	Debe ser compatible con NAT de destino;
		24	Debe soportar NAT de origen y NAT de destino de forma simultánea;
		25	Debe soportar NAT de origen y NAT de destino en la misma política
		26	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
		27	Debe ser compatible con NAT64 y NAT46;
		28	Debe implementar el protocolo ECMP;
		29	Debe soportar SD-WAN de forma nativa
		30	Debe soportar el balanceo de enlace hash por IP de origen;
		31	Debe soportar el balanceo de enlace por hash de IP de origen y destino;
		32	Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
		33	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
		34	Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
		35	Enviar logs a sistemas de gestión externos simultáneamente;
		36	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
		37	Debe soporta protección contra la suplantación de identidad (anti-spoofing);
		38	Implementar la optimización del tráfico entre dos dispositivos;
		39	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
		40	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
		41	Soportar OSPF graceful restart;
		42	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico

			de datos de la red;
		43	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
		44	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
		45	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
		46	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
		47	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
		48	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster;
		49	La configuración de alta disponibilidad debe sincronizar: Sesiones;
		50	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
		51	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
		52	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
		53	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
		54	Debe soportar la creación de sistemas virtuales en el mismo equipo;
		55	Para una alta disponibilidad, el uso de clústeres virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
		56	Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
		57	La plataforma de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;

		58	Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
		59	Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
		60	El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
		61	Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;
		62	La consola de administración debe soportar como mínimo, inglés y español.
		63	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad.
		64	El equipo debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
		B. Control de política por Firewall	
		1	Debe soportar controles de zona de seguridad;
		2	Debe contar con políticas de control por puerto y protocolo;
		3	Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
		4	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
		5	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
		6	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;

		7	Debe soportar automatización de situaciones como detención de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
		8	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
		9	Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.
		10	Debe soportar el protocolo estándar de la industria VXLAN;
		11	La solución debe permitir la implementación sin asistencia de SD-WAN.
		12	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
		13	la solución debe soportar la integración nativa con plataforma de sandboxing, protección de correo electrónico, cache y Web application firewall.
		C. Control de Aplicación	
		1	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
		2	Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
		3	Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
		4	Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;

		5	Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
		6	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
		7	Actualización de la base de firmas de la aplicación de forma automática;
		8	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
		9	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
		10	Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
		11	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
		12	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc.) permitiendo granularidad de control/reglas para el mismo;
		13	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
		14	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat pero impedir la llamada de video;
		15	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
		16	Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc.);
		17	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación;
		18	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de estas, tales como: Categoría de Aplicación;
		19	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

		D. Prevención de Amenazas	
		1	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
		2	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
		3	Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
		4	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
		5	Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
		6	Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
		7	Debe incluir la protección contra ataques de denegación de servicio;
		8	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
		9	Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
		10	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
		11	Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;
		12	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
		13	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP UDP, etc.
		14	Detectar y bloquear los escaneos de puertos de origen;
		15	Bloquear ataques realizados por gusanos (worms) conocidos;
		16	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;

		17	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
		18	Debe poder crear firmas personalizadas en la interfaz gráfica de la solución;
		19	Identificar y bloquear la comunicación con redes de bots;
		20	Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
		21	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
		22	Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
		23	Los eventos deben identificar el país que origino la amenaza;
		24	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
		25	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
		26	Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
		27	En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc.) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;

		28	Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);
		E. Identificación de Usuarios	
		1	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
		2	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / controles basados en usuarios y grupos de usuarios;
		3	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.;
		4	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;
		5	Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;
		6	Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
		7	Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
		8	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;

		9	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la Solución;
		10	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;
		F. Manejo de Tráfico (Traffic Shaping)	
		1	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
		2	Soportar la creación de políticas de QoS y Manejo de Tráfico por dirección de origen;
		3	Soportar la creación de políticas de QoS y Manejo de Tráfico por dirección de destino;
		4	Soportar la creación de políticas de QoS y Manejo de Tráfico por usuario y grupo;
		5	Soportar la creación de políticas de QoS y Manejo de Tráfico para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
		6	Soportar la creación de políticas de calidad de servicio y Manejo de Tráfico por puerto;
		7	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
		8	En QoS debe permitir la definición de tráfico con máximo ancho de banda;
		9	En QoS debe permitir la definición de colas de prioridad;
		10	Soportar marcación de paquetes DiffServ, incluso por aplicación;
		11	Soportar la modificación de los valores de DSCP para Diffserv;
		12	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
		13	Debe soportar QoS (manejo de tráfico o traffic-shaping) en las interfaces agregadas o redundantes;
		G. VPN	
		1	Soporte VPN de sitio-a-sitio y cliente-a-sitio;
		2	Soportar VPN IPSec;
		3	Soportar VPN SSL;
		4	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512

		5	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
		6	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
		7	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
		8	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
		9	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
		10	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
		11	Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
		12	Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
		13	Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
		14	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
		15	Deberá mantener una conexión segura con el portal durante la sesión;
		16	El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.
		H. Accesorios Incluidos	
			Cada firewall debe entregarse con 2 interfaces con el SFP+, Multimodo ya instalado y la misma cantidad de cordones de parcheo de fibra óptica certificados .

4.3

Módulo	Clasificación Funcional		Descripción de la Función
Dos (2) Dispositivos Next Generation Firewall para protección de Perímetro	Firewall Perimetral	1	Puerto de administración dedicada, fuera de banda o similar de tipo RJ45
		2	Puerto de consola serial
		3	16 puertos GE RJ45
		4	8 puertos GE SFP
		5	12 puertos 25GE SFP28 o 10 GE SFP+
		6	4 puertos 40 GE QSFP+

		7	Rendimiento de IPS 17 Gbps
		8	Rendimiento de NGFW 11 Gbps
		9	Rendimiento de protección de amenazas 9 Gbps
		10	Rendimiento de inspección SSL 12 Gbps
		11	Latencia de Firewall 4 microsegundos
		12	Rendimiento de Firewall de 200 Mpps
		13	Sesiones concurrentes TCP 8 millones como mínimo
		14	Nuevas sesiones/segundo 500,000
		15	Políticas de Firewall 10,000 como mínimo
		16	Rendimiento de control de aplicaciones 24 Gbps
		17	El equipo debe ser líder en el cuadrante mágico de Gartner para WAN Edge y Network Firewalls.
		18	El equipo debe ser compatible con la plataforma de logs y gestión de Firewalls actualmente en el Instituto.
		19	Soporte para la creación de dominios virtuales
		20	Soporte de alta disponibilidad en modos Activo-Activo, Activo-Pasivo y Clustering
		21	2 unidades de rack con kit de montaje y tornillos incluidos para su instalación
		22	Fuentes de poder intercambiables en caliente (hot-swap) y redundantes 100-240V AC, 50-60Hz
		A. Funcionalidades Generales	
		1	Los equipos deben consistir en una Solución de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;
		2	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;
		3	Las funcionalidades de protección de red que conforman la Solución de seguridad pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;
		4	La Solución debe estar optimizada para análisis de contenido de aplicaciones en capa 7;
		5	Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;
		6	La gestión de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;
		7	Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
		8	Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;
		9	Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;
		10	Los dispositivos de protección de red deben soportar

			encaminamiento de multicast (PIM-SM y PIM-DM);
		11	Los dispositivos de protección de red deben soportar DHCP Relay;
		12	Los dispositivos de protección de red deben soportar DHCP Server;
		13	Los dispositivos de protección de red deben soportar sFlow;
		14	Los dispositivos de protección de red deben soportar Jumbo Frames;
		15	Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
		16	Debe ser compatible con NAT dinámica (varios-a-1);
		17	Debe ser compatible con NAT dinámica (muchos-a-muchos);
		18	Debe soportar NAT estática (1-a-1);
		19	Debe admitir NAT estática (muchos-a-muchos);
		20	Debe ser compatible con NAT estático bidireccional 1-a-1;
		21	Debe ser compatible con la traducción de puertos (PAT);
		22	Debe ser compatible con NAT Origen;
		23	Debe ser compatible con NAT de destino;
		24	Debe soportar NAT de origen y NAT de destino de forma simultánea;
		25	Debe soportar NAT de origen y NAT de destino en la misma política;
		26	Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;
		27	Debe ser compatible con NAT64 y NAT46;
		28	Debe implementar el protocolo ECMP;
		29	Debe soportar SD-WAN de forma nativa;
		30	Debe soportar el balanceo de enlace hash por IP de origen;
		31	Debe soportar el balanceo de enlace por hash de IP de origen y destino;
		32	Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;
		33	Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;
		34	Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;

		35	Enviar logs a sistemas de gestión externos simultáneamente;
		36	Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
		37	Debe soporta protección contra la suplantación de identidad (anti-spoofing);
		38	Implementar la optimización del tráfico entre dos dispositivos;
		39	Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
		40	Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
		41	Soportar OSPF graceful restart;
		42	Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
		43	Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
		44	Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
		45	Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
		46	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
		47	Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
		48	Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
		49	La configuración de alta disponibilidad debe sincronizar: Sesiones;
		50	La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando políticas de Firewalls, NAT, QoS y objetos de la red;
		51	La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
		52	La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
		53	En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
		54	Debe soportar la creación de sistemas virtuales en el mismo equipo;
		55	Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;

		56	Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
		57	La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
		58	Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
		59	Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
		60	El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
		61	Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;
		62	La consola de administración debe soportar como mínimo, inglés y español.
		63	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad
		64	La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
		B. Control de política por Firewall	
		1	Debe soportar controles de zona de seguridad;
		2	Debe contar con políticas de control por puerto y protocolo;
		3	Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
		4	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
		5	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
		6	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse

			directamente a las políticas de firewall;
		7	Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
		8	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
		9	Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
		10	Debe soportar el protocolo estándar de la industria VXLAN;
		11	La solución debe permitir la implementación sin asistencia de SD-WAN
		12	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
		13	Los equipos deben soportar la integración nativa con plataforma de sandboxing, protección de correo electrónico, cache y Web application firewall.
		C. Control de Aplicación	
		1	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
		2	Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
		3	Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
		4	Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;

		5	Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;
		6	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
		7	Actualización de la base de firmas de la aplicación de forma automática;
		8	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
		9	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
		10	Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
		11	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
		12	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc.) permitiendo granularidad de control/reglas para el mismo;
		13	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
		14	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat, pero impedir la llamada de video;
		15	Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
		16	Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de estas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc.);
		17	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de estas, tales como: Nivel de riesgo de la aplicación;
		18	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de estas, tales como: Categoría de Aplicación;
		19	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente
		D. Prevención de Amenazas	
		1	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
		2	Debe incluir firmas de prevención de intrusiones (IPS) y

			el bloqueo de archivos maliciosos (antivirus y anti-spyware);
		3	Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
		4	Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
		5	Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
		6	Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
		7	Debe incluir la protección contra ataques de denegación de servicio;
		8	Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
		9	Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
		10	Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
		11	Debe tener los siguientes mecanismos de inspección IPS: Reensamblado de paquetes TCP;
		12	Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
		13	Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.;
		14	Detectar y bloquear los escaneos de puertos de origen;
		15	Bloquear ataques realizados por gusanos (worms) conocidos;
		16	Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
		17	Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
		18	Debe poder crear firmas personalizadas en la interfaz gráfica de la solución;
		19	Identificar y bloquear la comunicación con redes de bots;
		20	Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;

		21	Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
		22	Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
		23	Los eventos deben identificar el país que origino la amenaza;
		24	Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
		25	Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
		26	Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
		27	En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc.) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
		28	Proporcionar protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);
		E. Filtrado URL	
		1	Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
		2	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
		3	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
		4	Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
		5	Tener por lo menos 75 categorías de URL;
		6	Debe tener la funcionalidad de exclusión de URLs por categoría;
		7	Permitir página de bloqueo personalizada;

		8	Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
		9	Además del Explicit Web Proxy, soportar proxy web transparente;
		F. Identificación de Usuarios	
		1	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
		2	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas/controles basados en usuarios y grupos de usuarios;
		3	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límite de usuarios licenciados o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.;
		4	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basado en usuarios y grupos de usuarios;
		5	Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;
		6	Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
		7	Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
		8	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
		9	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la Solución;
		10	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;

		G. Manejo de Tráfico (Traffic Shaping)	
		1	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, tenga la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
		2	Soportar la creación de políticas de QoS y Manejo de Tráfico por dirección de origen;
		3	Soportar la creación de políticas de QoS y Manejo de Tráfico por dirección de destino;
		4	Soportar la creación de políticas de QoS y Manejo de Tráfico por usuario y grupo;
		5	Soportar la creación de políticas de QoS y Manejo de Tráfico para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
		6	Soportar la creación de políticas de calidad de servicio y Manejo de Tráfico por puerto;
		7	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
		8	En QoS debe permitir la definición de tráfico con máximo ancho de banda;
		9	En QoS debe permitir la definición de colas de prioridad;
		10	Soportar marcación de paquetes DiffServ, incluso por aplicación;
		11	Soportar la modificación de los valores de DSCP para Diffserv;
		12	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
		13	Debe soportar QoS (Manejo de tráfico o traffic-shaping) en las interfaces agregadas o redundantes;
		H. VPN	
		1	Soporte VPN de sitio-a-sitio y cliente-a-sitio;
		2	Soportar VPN IPSec;
		3	Soportar VPN SSL;
		4	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
		5	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
		6	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
		7	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
		8	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

		9	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
		10	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting;
		11	Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
		12	Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
		13	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
		14	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
		15	Deberá mantener una conexión segura con el portal durante la sesión;
		16	El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.
		I. Accesorios Incluidos	
			Cada firewall debe entregarse con 2 interfaces SFP+, Multimodo ya instalado y la misma cantidad de cordones de parcheo de fibra óptica certificados.

4.4 El EQUIPO debe incluir las siguientes funcionalidades y software, como se describe a continuación:

		Funcionalidades para integrar	
		Debe integrar una solución de Protección de correo electrónico, Antispam.	
			Debe ser una solución basada en la nube para 13,000 cuentas
			Debe contar con esquema de HA brindado por el fabricante de la solución
			Debe tener escalabilidad, es decir permitir el escalamiento de buzones de correo.
			La institución no se debe preocupar por temas de infraestructura siendo una solución SaaS
			La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.
			La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent).

			La solución debe ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidas.
			Debe poder ser instalado en forma de proxy SMTP transparente, para el análisis de correo saliente, buscando evitar el reporte en Blacklist
			Debe tener disponible un API basado en REST para fines de monitoreo, automatización y orquestación.
			El licenciamiento debe ser basado por cantidad de buzones a proteger.
		A. **Funcionalidades Generales**	
			La solución debe soportar listas blancas y negras (White/Black List) por usuario, por dominio y globalmente para todo el sistema.
			La solución debe permitir la sobreescritura, la edición y personalización de los mensajes de notificación de antivirus y anti-spyware.
			La solución debe poder retrasar el envío de correo sobredimensionados a horarios que sean de menos carga.
			La solución debe poder definir el reenvío de correo (relay) a una Ip especifica con base a la IP origen del mensaje.
			La solución debe proporcionar soporte para múltiples dominios de correo electrónico.
			La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente
			La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.
			La solución debe soportar cuarentena por usuario, permitiendo que cada usuario puede gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo. La cuarentena se debe acceder a través de la página web y POP3.
			La solución debe ser capaz de programar el envío de informes de cuarentena.

			La solución debe ser capaz de mantener la cola de correo (Queue) en caso de fallo en la conexión de salida, retrasos o errores de entrega.
			La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP.
			La solución debe ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados.
			La solución debe ser compatible con el enrutamiento en IPv4 y IPv6.
			La solución debe permitir el almacenamiento de correo electrónico y de cuarentena a nivel local o servidor remoto.
			La solución debe tener características antispam, antivirus, anti-spyware y anti-phishing.
			La solución debe ser capaz de realizar la inspección del correo de Internet entrante y saliente.
			La solución debe contar con un Asistente (Wizard) para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger
			La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb.
			La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing.
		B. **Funcionalidades de Antispam**	
			La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam.
			La solución puede detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante.
			La solución puede detectar si un correo es spam revisando las URLs que esta contenga, comparándolas con la base de datos de reputación suministrada por el fabricante.

			La revisión de URLs debe permitir seleccionar las categorías URL que serán permitidas o no en los correos analizados. Esta base de datos de categorías será actualizada por el fabricante.
			La solución debe contar con mecanismos de detección de SPAM nuevo, mediante el análisis continuo de los correos recibidos y su posterior correlación con eventos ocurridos a nivel mundial, permitiendo así definir y detectar nuevas reglas de SPAM
			La solución debe ser capaz de realizar análisis Heurístico y definir umbrales máximos de acuerdo con el comportamiento del correo y así determinar si un correo es spam.
			La solución debe ser capaz de realizar análisis Bayesiano para determinar si un correo es spam.
			La solución debe ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter).
			La solución debe contar con técnica que detecten SPAM mediante el uso de Greylist, las cuales clasifican el correo con base en su comportamiento en el inicio de sesión, como bloquear todos los correos y permitir solo los reenvíos.
			La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words).
			La solución debe contar con Diccionarios predefinidos de palabras que pueden ser escaneados en el correo electrónico, además definir pesos a cada diccionario o palabra creada para definir si un correo es SPAM.
			La solución permite crear lista blancas o negras de palabras.
			La solución debe permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal, sobre escribir el destinatario, Archivar, enviar copia oculta BCC, reenviar a otro Host, Insertar un TAG o un nuevo encabezado.
			La solución debe ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM.

			La solución debe ser capaz de soportar las listas negras de terceros tales como DNSBL y SURBL.
			La solución debe ser capaz de detectar las direcciones IP falsificadas (Forged IP).
			La solución permite identificar imágenes que hagan alusión a contenido SPAM. Debe soportar el análisis de las siguientes extensiones GIF, JPEG, PNG.
		C. Funcionalidades de Sesion	
			La solución debe poder validar si el destinatario del correo entrante es un buzón válido
			La solución debe ser compatible con Sender Policy Framework (SPF).
			La solución debe ser compatible con Domain Keys Identified Mail (DKIM).
			La solución debe ser compatible con Domain Based Message Authentication (DMARC).
			La solución debe identificar altos volúmenes de conexiones y aplicar limites basado en senders e Ips.
			La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico.
		D. **Funcionalidades de gestion**	
			La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS).
			La solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.
			La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only)
			La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como anti-spam, anti-virus, autenticación, entre otros.
			La solución debe soportar doble factor de autenticación para el login de usuarios administradores

		E. **Funcionalidades de DLP**	
			También debe proporcionar una plataforma DLP para detectar la información sensible que puede estar llegando por e-mail.
			La funcionalidad DLP debe permitir definir la información a detectar como palabras, frases y expresiones regulares.
			La funcionalidad DLP debe tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros.
			La funcionalidad DLP debe permitir la creación y almacenamiento de impresiones digitales (Fingerprint) de documentos.
			La funcionalidad DLP para permitir la creación de filtros por tipos de archivos;
			La funcionalidad DLP debe permitir la generación y almacenamiento de impresiones digitales (fingerprints) de los archivos adjuntos de correo electrónico.
			La funcionalidad DLP debe permitir el almacenamiento de impresiones digitales (Fingerprints) de archivos antiguos y también para los nuevos archivos que se han actualizado.
		F. **Funcionalidades de Cifras**	
			Debe soportar Cifrado de mensajes basado en identidad (IBE- Identity Based Encryption), de tal forma que el destinatario no requiera de un PSK o certificado previamente instalado para su descifrado
			En ambos métodos de cifrado con IBE se debe contar con un registro del destinatario en la plataforma de correo, de tal forma que para ver los mensajes cifrados se requiera un proceso de autenticación.
			Debe soportar cifrado de correo usando S/MIMEc
			Debe soportar cifrado SMTPS y SMTP over TLS.
		G. **Funcionalidades de Regulación**	
			La solución debe analizar el contenido y adjuntos de un mensaje en busca de palabras que indiquen que el correo deba ser puesto en cuarentena, Cifrado, Archivado, Bloqueado,

			Taggeado, sobrescrito o reenviado a otro host.
			Debe contar con Diccionarios predefinidos que permitan el cumplimiento de normativas como HIPAA, GLB, SOX, estos diccionarios debe identificar: Canadian SIN, US SSN, Credit card, ABA Routing, CUSIP, ISIN y poder definir diccionarios personalizados.
			Debe poder inspeccionar archivos protegidos por contraseña, mediante password predefinidos, una lista de contraseñas o buscar en el cuerpo la palabra password.
		H. **Funcionalidades de Log y Reportería**	
			La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog).
			La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.
			La solución debe generar informes por demanda o programados a intervalos de tiempo específicos
			La solución debe generar y enviar informes en formato PDF o HTML.
		I. **RFCs Soportadas**	
			Debe soportar el RFC 1213 (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II)
			Debe soportar el RFC 1918 (Address Allocation for Private Internets)
			Debe soportar el RFC 1985 (SMTP Service Extension for Remote Message Queue Starting)
			Debe soportar el RFC 2034 (SMTP Service Extension for Returning Enhanced Error Codes)
			Debe soportar el RFC 2045 (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies)
			Debe soportar el RFC 2505 (Anti-Spam Recommendations for SMTP MTAs)
			Debe soportar el RFC 2634 (Enhanced Security Services for S/MIME)

			Debe soportar el RFC 2920 (SMTP Service Extension for Command Pipelining)
			Debe soportar el RFC 3207 (SMTP Service Extension for Secure SMTP over TLS)
			Debe soportar el RFC 3461 (SMTP Service Extension for Delivery Status Notifications DSNs)
			Debe soportar el RFC 3463 (Enhanced Mail System Status Codes)
			Debe soportar el RFC 3464 (Extensible Message Format for Delivery Status Notifications)
			Debe soportar el RFC 3635 (Definitions of Managed Objects for the Ethernet-like Interface Types)
			Debe soportar el RFC 4954 (SMTP Service Extension for Authentication)
			Debe soportar el RFC 5321 (SMTP)
			Debe soportar el RFC 5322 (Internet Message Format)
			Debe soportar el RFC 6376 (DomainKeys Identified Mail (DKIM) Signatures)
			Debe soportar el RFC 6522 (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages)
			Debe soportar el RFC 6409 (Message Submission)
			Debe soportar el RFC 7208 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail)
			Debe soportar el RFC 2088 (IMAP4 Non-synchronizing Literals)
			Debe soportar el RFC 2177 (IMAP4 Idle Command)
			Debe soportar el RFC 2221 (Login Referrals)
			Debe soportar el RFC 2342 (IMAP4 Namespace)
			Debe soportar el RFC 2683 (IMAP4 Implementation Recommendations)
			Debe soportar el RFC 2971 (IMAP4 ID Extension)
			Debe soportar el RFC 3348 (IMAP4 Child Mailbox Extension)

			Debe soportar el RFC 3501 (IMAP4 rev1)
			Debe soportar el RFC 3502 (IMAP Multiappend Extension)
			Debe soportar el RFC 3516 (IMAP4 Binary Content Extension)
			Debe soportar el RFC 3691 (Unselect Command)
			Debe soportar el RFC 4315 (UIDPLUS Extension)
			Debe soportar el RFC 4469 (Catenate Extension)
			Debe soportar el RFC 4731 (Extension to SEARCH Command for Controlling What Kind of Information Is Returned)
			Debe soportar el RFC 4959 (Extension for Simple Authentication and Security Layer (SASL) Initial Client Response)
			Debe soportar el RFC 5032 (WITHIN Search Extension)
			Debe soportar el RFC 5161 (Enable Extension)
			Debe soportar el RFC 5182 (Extension for Referencing the Last SEARCH Result)
			Debe soportar el RFC 5255 (IMAP Internationalization)
			Debe soportar el RFC 5256 (Sort and Thread Extensions)
			Debe soportar el RFC 5258 (List Command Extensions)
			Debe soportar el RFC 5267 (Contexts for IMAP4)
			Debe soportar el RFC 5819 (Extension for Returning STATUS Information in Extended LIST)
			Debe soportar el RFC 6154 (LIST Extension for Special-Use Mailboxes)
			Debe soportar el RFC 6851 (MOVE extension)
			Debe soportar el RFC 7162 (IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC))
			Debe soportar el RFC 1939 (POP3)
			Debe soportar el RFC 2449 (POP3 Extension Mechanism)

			Debe soportar el RFC 1155 (Structure and Identification of Management Information for TCP/IP-based Interface)
			Debe soportar el RFC 1157 (SNMP v1)
			Debe soportar el RFC 1213 (MIB 2)
			Debe soportar el RFC 2578 (Structure of Management Information Version 2)
			Debe soportar el RFC 2579 (Textual Conventions for SMIv2)
			Debe soportar el RFC 2595 (Using TLS with IMAP, POP3 and ACAP)
			Debe soportar el RFC 3410 (SNMP v3)
			Debe soportar el RFC 3416 (SNMP v2)

4.4.1

		Funcionalidades para integrar	
		Protección avanzada contra amenazas persistentes "Sandbox"	
		La cual tendrá como función principal la detonación Remota de amenazas de día Cero.	
		A. Deberá contener las siguientes características	
		1	Soporte para 22 máquinas virtuales para pruebas de sandbox como mínimo, entre ellas Windows 8, Windows 10 y 5 licencias de Office.
		2	Soporte para inteligencia de amenazas como Antivirus, IPS, Web Filtering, File query y seguridad industrial.
		3	4 interfaces de 1Gbps RJ-45
		4	2 interfaces de 10Gbps SFP+
		5	2 discos de 1 TB
		6	Fuentes de poder intercambiables en caliente (hot-swap) y redundantes
		B. Funciones de protección generales	
		1	El dispositivo deberá tener la capacidad de inspeccionar el tráfico entrante en busca de malware desconocido de los tipos: Advanced Persistent Threat, Zero-Day Threats y ramsonware con filtros de amenazas avanzadas y análisis de ejecución en tiempo real e inspección del tráfico saliente.
		2	El dispositivo de protección debe poder enviar tráfico de archivos automáticamente para su análisis en El dispositivo instalada localmente (on-premise), donde el archivo se ejecutará y simulará en un entorno controlado.

		3	El dispositivo debe admitir la supervisión de trafico de archivos en Internet (HTTP, FTP, HTTPS, SMTP), así como tráfico de archivos internamente entre servidores de archivos que usan SMB en todos los modos de implementación: sniffer, transparente y L3.
		4	El dispositivo debe poder analizar tráfico cifrado SSL.
		5	El dispositivo debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos.
		6	El dispositivo debe permitir la selección a través de políticas para indicar qué tipos de archivos se someterán a análisis y prevención.
		7	El dispositivo debe poder identificar la existencia de malware en archivos adjuntos de correo electrónico y URL conocidas.
		C. Funciones de Protección contra Amenazas Persistentes	
		1	Debe contar con detección inmediata y bloqueo de malware que utiliza mecanismos de escaneo en archivos PDF.
		2	El dispositivo debería proporcionar la capacidad de emular ataques en sistemas operativos y aplicaciones siguientes: - Windows 7 - Windows 8.1 - Windows 10 - MacOS - Android
		3	Soporte de análisis de sandbox para archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android, MacOS y Linux.
		4	El fabricante del dispositivo debe tener una nube de inteligencia que de actualice toda la base de seguridad mediante firmas.
		5	El dispositivo debe admitir topologías de implementación con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP o BCC.
		6	El dispositivo debe admitir topologías de implementación mediante el intercambio de archivos
		7	El dispositivo debe admitir topologías de implementación bajo demanda
		8	El dispositivo debe admitir topologías de implementación a través de la API JSON
		9	El dispositivo debe permitir la carga de máquinas virtuales personalizadas.
		10	Todos los análisis y bloqueos de malware y / o códigos maliciosos deben realizarse en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo

			detecten malware y / o códigos maliciosos
		11	El dispositivo debe admitir las reglas de YARA como estándar para crear reglas para la detección de malware
		12	Permita la creación de firmas en tiempo real para las amenazas detectadas mediante el análisis del comportamiento en el entorno limitado con la distribución de la firma local entre los dispositivos integrados, como firewall, email secure gateway, endpoint o web application Firewall. Por lo tanto, todos los dispositivos integrados en El dispositivo de sandbox están inmediatamente protegidos contra nuevas amenazas.
		D. Funciones de Visibilidad:	
		1	Debe permitir al administrador del dispositivo descargar el archivo original, analizado por la plataforma de sandbox
		2	En caso de encontrar una amenaza positiva el equipo debe presentar la siguiente información detallada, para fines de auditoría, sobre el comportamiento comprometido de la máquina:
		3	Tipo de archivo: o IP de la fuente del malware o IP de destino (cliente que descargó el malware) o Link de referencia hacia descarga del malware o Resumen del comportamiento del malware en la máquina virtual comprometida

4.4.2

		Control de Accesos a la Red "NAC"	
		Debe tener la funcionalidad del permitir el control de acceso a la red y perfilamiento de dispositivos	
		1	La solución debe contar con las licencias en su implementación para al menos, 15,000 dispositivos conectados simultáneamente, estas deben ser perpetuas.
		2	Debe ser del tipo VM, compatible con el hipervisor del Instituto, permitiendo el uso de 20 vCPU y 32 GB de memoria RAM.
		3	La solución debe ser escalable, permitiendo instalaciones de múltiples dispositivos físicos adicionales coordinados para crecimiento.
		4	La solución debe permitir el crecimiento mediante la compra de licencias por cantidad de dispositivos y estas deben ser perpetuas y permitir distintos niveles de operación (visibilidad, control, cumplimiento).
		A. Visibilidad a nivel de Red	
		1	Permitir un despliegue centralizado, en una arquitectura fuera de banda.

		2	Brindar control de acceso en Capa 2 sobre una infraestructura cableada e inalámbrica.
		3	Permitir crear una estructura jerárquica que permita ordenar los dispositivos de infraestructura de la red de manera lógica o geográfica.
		4	Permitir crear, modificar y borrar dispositivos y sus características.
		5	Permitir el registro manual de dispositivos sin soporte SNMP.
		6	Contar con un proceso continuo de detección y categorización de dispositivos de infraestructura de red, que permita detectar y controlar los switches, routers y otros dispositivos de la red.
		7	Permitir mover los dispositivos dentro de la estructura jerárquica generada.
		8	Permitir realizar polling de los dispositivos en capa 2.
		9	La solución debe operar indistintamente para entornos cableados o inalámbricos, en capa 2 o capa 3.
		B. Visibilidad a Nivel de Endpoint	
		1	Permitir la detección de hosts desconocidos.
		2	Permitir la identificación de hosts mediante Portal Cautivo.
		3	Permitir la categorización automática de hosts.
		4	Mantener el perfil asignado a cada host, y verificar que sigue siendo válido en cada nueva conexión del host. Si el perfil variara, deberá impedir su conexión y notificar inmediatamente sobre el hecho.
		5	Permitir la fijación de períodos de tiempo en los que el host está autorizado a operar, y evaluarlos periódicamente.
		6	Permitir la importación de un archivo .CSV conteniendo información sobre los hosts a registrar.
		7	Permitir la integración con plataformas MDM.
		8	Permitir determinar el perfil de los hosts descubiertos mediante métodos que no requieran la instalación de agentes incluyendo, al menos, los siguientes: - DHCP Fingerprinting - HTTP/HTTPS - Ubicación - SNMP - SSH - Telnet - TCP - UDP - OUI - WMI - WinRM

		9	Poder reconocer los siguientes sistemas operativos sin necesidad de agentes: - Android - Apple iOS for iPhone/iPad7/iPod - Blackberry OS/Blackberry 10 OS - Chrome OS - Free BSD - Kindle/Kindle Fire - Linux - Mac OS X - Open BSD - Solaris - Symbian - Web OS - Windows - Windows Phone/CE/RT
		10	El dispositivo no debe requerir el uso de 802.1x para permitir el descubrimiento de hosts o usuarios, o brindar control de acceso a nivel de Puerto en la infraestructura alámbrica.
		C. Visibilidad a nivel de usuario	
		1	Permitir la identificación de usuarios mediante Active Directory.
		2	Permitir la identificación de usuarios mediante Portal Cautivo.
		3	Incluir opciones de análisis flexibles para plataformas Windows, MacOS y Linux. La tecnología de agentes desvanecibles no debe requerir la instalación de software de terceros, tales como Java.
		4	Permitir la designación de un sponsor que autorice el acceso de un invitado.
		5	Permitir la designación de un sponsor que autorice la categorización de un host
		D. Funciones de automatización y control requeridas	
		1	Debe permitir el ingreso de credenciales mediante 802.1x o Portal Cautivo.
		2	Soportar la validación de credenciales: Servidor RADIUS Servidor LDAP
		3	Debe soportar la validación automática de credenciales mediante agentes persistentes o volátiles.
		4	La solución debe tener la capacidad de aprovechar la combinación de informaciones sobre la identidad del usuario y el tipo de dispositivo para aprovisionar dinámicamente permisos de acceso basados en roles y distintos niveles de acceso.
		5	Debe permitir la generación de políticas de control, agrupadas jerárquicamente, y determinar la política a aplicar a cada dispositivo en función de una serie de reglas de asignación.

		6	Debe soportar, al menos, los siguientes tipos de información para determinar la política a aplicar: - Ubicación - Grupo de Pertenencia - Atributo - Fecha y Hora
		7	La solución debe incluir funcionalidades de Guest Management, permitiendo la creación de perfiles de Invitados.
		8	Debe permitir la creación de plantillas que agrupen a los invitados en grupos que tengan distintos permisos de acceso, o períodos de tiempo de acceso permitido.
		9	Debe contar con herramientas que permitan la generación y mantenimiento de este tipo de usuarios y sus claves de acceso.
		10	Debe permitir la creación de Portales de Auto-Registro.
		11	Debe permitir la existencia de Sponsors que aprueben el ingreso de Invitados a la red, o que eleven los permisos de acceso de ciertos individuos.
		12	La solución debe incluir funcionalidades de IoT Onboarding con autorización de Sponsors.
		13	La solución debe incluir funcionalidades de Endpoint Compliance. Antes de permitir el acceso de los dispositivos a la red, debe asegurarse de que estos cumplen con una serie de requisitos de seguridad, integridad y configuración, que hagan seguro su acceso a la red.
		14	Debe permitir el uso de agentes persistentes, evanescentes (desaparecen luego de realizado en análisis) o pasivos.
		15	Si un dispositivo no pasa los tests de Compliance, debe ser posible: - No forzar la remediación - Forzar la remediación inmediatamente, enviando al dispositivo a una red de cuarentena - Permitir la remediación retardada, dando un período de tiempo desde la detección inicial de problemas, para la solución de estos. Pasado el período de tolerancia, de persistir los problemas, el dispositivo debe ser puesto en cuarentena inmediatamente.
		E. Respuesta a Incidentes	
		1	Debe permitir la construcción de reglas de seguridad que se activen ante eventos de seguridad definidos por el administrador y generar alarmas de seguridad.
		2	Ante una alarma de seguridad debe permitir el bloqueo o aislamiento automático de los hosts comprometidos.
		3	Debe permitir la creación, modificación y borrado de acciones que puedan ser asociadas a una alarma.

		4	Las acciones por ejecutar deben incluir, al menos: - Ejecución de un script de comandos - Enviar una alarma a un log externo - Enviar un mensaje de correo electrónico al usuario o a los administradores - Cambiar el rol del host involucrado - Deshabilitar el host - Deshabilitar el puerto de conexión - Revalidar el estado de compliance del host - Marcar el host como En Riesgo - Marcar el host como Seguro
		F. Integración requerida con otras soluciones	
		1	El dispositivo debe tener la capacidad de interoperar con dispositivos de conexión cableada e inalámbrica de los principales fabricantes, incluyendo, como mínimo: - Cisco/Meraki - HP/HP Procurve/3Com/Aruba - Extreme Networks/Enterasys/Motorola/Avaya/Brocade - Fortinet - Juniper - Dell - Alcatel-Lucent - D-Link - Huawei - Ruckus
		2	El dispositivo debe permitir la integración de dispositivos de infraestructura de seguridad de terceras partes instaladas actualmente en la institución: - Cisco ASA - Fortinet - SonicWall
		3	La solución debe permitir la integración de Servicios de Directorios y Sistemas Operativos, incluyendo: - RADIUS: Microsoft IAS, - LDAP: Microsoft Active Directory, OpenLDAP - Microsoft Windows - Apple Mac OS X e IOS - Linux - Android
		4	La solución debe permitir la integración de Aplicaciones de Seguridad de Endpoints, incluyendo: - ESET (Instalado actualmente en la Institución) - Kaspersky - McAffee - Microsoft - Norton - Sophos - Symantec - Trend Micro

		5	La solución debe contar con un método genérico de integración de dispositivos, mediante la recepción, análisis e interpretación de mensajes de Syslog.
		6	La solución debe incluir una REST API que permita:
		7	Obtener información detallada sobre un elemento en particular, tal como un usuario o un host.
		8	Interrogar a la base de datos para obtener información sobre un conjunto de dispositivos
		9	Actualizar los registros de usuarios o dispositivos
		10	Bloquear o desbloquear el acceso de un usuario o dispositivo a la red
		G. Gestión de NAC	
		1	La solución debe permitir distintos roles administrativos, incluyendo la capacidad de limitar y controlar la cantidad de acceso permitido a las funcionalidades disponibles, dependiendo del grupo administrativo de la organización al que pertenezca el usuario. Por ej., Help Desk, Operaciones de Red, Operaciones de Seguridad.
		2	La solución debe proveer reportes de auditoría de todas las conexiones de la red, tanto cableadas como inalámbricas. Esto debe incluir una interfaz que permita buscar y generar consultas en la información almacenada.
		3	La solución debe incluir reportes de auditoría de todas las acciones y cambios realizados al sistema por los usuarios administradores, incluyendo qué se cambió, cuándo se cambió y quién lo cambió.
		H. Reportería que debe incluir la solución	
		1	Debe contar con un dashboard que presente información relevante de manera resumida.
		2	El dashboard debe poder ser modificable para permitir el despliegue de la información que el administrador considere más relevante.
		3	Debe contar con reportes predefinidos que incluyan resultados sobre:
		4	Registro de Invitados
		5	Registro de dispositivos
		6	Escaneo de Dispositivos
		7	Debe permitir la generación de reportes a medida sobre:
		8	Registro de usuarios y Dispositivos
		9	Falla en los Registros
		10	Logs de Conexión
		11	Debe permitir la generación y archivado de reportes periódicos.
		12	Debe permitir el envío automatizado de reportes mediante correo electrónico.
		13	Debe contar con reportes de Compliance de PCI.
		14	La información de los reportes debe poder ser

			exportada en formato HTML, CSV, Excel, XML, RTF o PDF.
		15	El log de alarmas debe poder ordenarse por severidad.
		16	Debe permitir la aceptación y eliminación de alarmas del log de forma manual.
		17	Debe permitir la aceptación y eliminación de alarmas del log de forma automática.
		18	Debe permitir la definición de alarmas en función de la ocurrencia de determinados eventos.

4.4.3

			Protección basada en señuelos para bloqueo de amenazas internas y externas "HoneyPot"
		Debe contener las siguientes características:	
		1	Los derechos de uso de licencia (protección contra amenazas basada en engaños) deberán tener una capacidad de 5 (cinco) VLANs (redes virtuales) y hasta 128 (ciento veintiocho) redes.
		2	Los derechos de uso de licencias (protección contra amenazas basada en engaños) deberán tener la capacidad de emular hasta 2(dos) instancias de máquinas virtuales del Sistema Operativo Windows 10 y 2 (dos) instancias de máquinas virtuales del sistema operativo Linux.
		3	Los derechos de uso de licencias (protección contra amenazas basada en engaños) deberán estar diseñados para engañar, exponer y eliminar ataques avanzados evitando que el programa maligno se propague, brindando visibilidad a la actividad maliciosa que puede haber pasado los controles de seguridad tradicionales automatizando la creación de máquinas virtuales engañosas llamadas señuelos para proporcionar una capa interna de protección para atraer y exponer a los atacantes que han penetrado en la red.
		4	El software de protección contra amenazas basada en engaños deberá engañar a las amenazas externas e internas con instancias de máquinas virtuales engañosas también conocidas como señuelos, administradas desde una ubicación centralizada siendo capaz de emular sistemas Windows, Linux, VPN, Medical IoT y SCADA con servicios que no se puedan distinguir de los activos reales, como: servidores de producción y señuelos integrados en dispositivos diseñados para descubrir a los atacantes.
		5	El software de protección contra amenazas basada en señuelos deberá exponer la actividad de los piratas informáticos con detección temprana y precisa, alertas procesables habilitadas a través del seguimiento y la correlación de las tácticas, herramientas y

			procedimientos de un atacante y la notificación activa a través de la interfaz de usuario web, correo electrónico, registros de logs y eventos a través de la infraestructura del instituto.
		6	El software de protección contra amenazas basada en señuelos deberá eliminar las amenazas detectadas mediante la automatización de la respuesta ante amenazas contra Firewalls, NAC y soluciones de seguridad de terceros a través la implementación del concepto de security mesh presentado por Gartner donde exista integración nativa y capacidades de automatización con otros elementos de la solución de ciberseguridad.
		7	El software de protección contra amenazas basadas en señuelos deberá soportar los siguientes servicios: SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP y TCP.
		8	El software de protección contra amenazas basado en señuelos deberá instalarse en una plataforma de hipervisor compatible con la infraestructura del instituto.

4.4.4

		Gestión y Monitoreo de la Solución de Ciberseguridad.	
		A. Arquitectura de la plataforma de gestión de la Solución de ciberseguridad.	
		1	Los derechos de uso del licenciamiento para el equipo propiedad del INSTITUTO, serán destinados para la orquestación y administración de equipos que se permita almacenar 1 TB de información, administrar 100 dispositivos de seguridad y recolectar 5 GB de logs. El licenciamiento que se deberá ofertar será utilizado para el despliegue de la máquina virtual en el hipervisor y administración de hasta 100 dispositivos de seguridad.
		2	Se requieren los derechos de uso del licenciamiento de tipo perpetuo para almacenar 1 TB de información, administrar 100 dispositivos de seguridad y recolectar 5 GB diarios de logs.
		3	Se debe contemplar agregar licenciamiento y soporte técnico por un plazo de tres (3) años, para la consola de orquestación y administración de equipos actualmente en uso incluyendo los 100 dispositivos agregados.
		B. Arquitectura de la plataforma de monitoreo, análisis y reportería de la Solución de ciberseguridad.	

		1	Debe incluir los derechos de uso del licenciamiento para el equipo propiedad del INSTITUTO mismos que serán destinados para generar reportes y realizar análisis de logs de las plataformas de seguridad. Los derechos de uso de la licencia deben permitir agregar capacidad a la plataforma con que ya cuenta el INSTITUTO.
		2	Se deben incluir los derechos de uso del licenciamiento perpetuo para almacenar 48TB de información y recolectar 500 GB diarios de logs.
		3	Debe soportar e incluir el servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: - Dirección IP de usuario - Nombre de host - Sistema operativo - Veredicto (clasificación general de la amenaza) - Número de amenazas detectadas.
		4	Se debe contemplar agregar licenciamiento y soporte técnico por un plazo de tres (3) años para la consola de análisis y reportes actualmente en uso, incluyendo la licencia que soporta los 500 GB de logs diarios a contratar en la presente adquisición.

4.4.5

		Gestión de Eventos e Incidentes de Seguridad – SIEM	
		Debe tener la funcionalidad de Monitoreo y correlación de incidentes de seguridad.	
		1	Debe ser del tipo VM, compatible con el Hipervisor del Instituto.
		2	Soporte para recepción de 18,000 EPS
		3	Soporte para 1600 dispositivos
		4	Soporte monitoreo y FIM para 200 servidores Windows
		5	Soporte monitoreo y FIM para 50 servidores Linux
		6	Soporte de IOC para 1600 dispositivos
		A. Requerimientos no funcionales	
		1	Interfaz gráfica basada en WEB
		2	Control de acceso basado en roles para restringir el acceso a la GUI y datos en varios niveles
		3	Toda la comunicación entre módulos debe estar protegida por protocolo HTTPS
		4	Seguimiento completo de auditoría de la actividad del usuario
		5	Actualizaciones de la base de conocimiento del fabricante (analizadores, reglas, informes)
		6	Archivo basado en políticas
		7	Hash de registros en tiempo real para no repudio e integridad verificación

		8	Autenticación de usuario flexible: local, externa a través de Microsoft AD y OpenLDAP, Cloud SSO / SAML a través de Okta
		9	Posibilidad de iniciar sesión en un servidor remoto detrás de un recopilador desde el GUI del equipo a través del túnel remoto SSH
		B. Requerimientos generales de la solución	
		1	Permite el descubrimiento y categorización de dispositivos de red, servidores, usuarios y aplicaciones en profundidad. Esta información alimenta una base de datos de administración de configuraciones (CMDB), la cual se mantiene actualizada por medio de redescubrimientos programados
		2	Debe poseer un lenguaje de análisis de registro basado en XML, flexible y computacionalmente eficiente.
		3	Debe recopilar sin problemas una gran variedad de métricas de rendimiento y disponibilidad para ayudar al investigador a buscar amenazas. También debe alertar cuando las métricas están fuera del perfil normal y puede correlacionar tales violaciones con problemas de seguridad para crear alertas de alta fidelidad.
		4	Debe proporcionar mecanismos para rastrear y detectar cambios de archivos clave. Debe monitorear la configuración de inicio y ejecución de dispositivos de red a través de SSH. Debe monitorear archivos de configuración en servidores. Debe monitorear eficientemente grandes infraestructuras de servidores. Crear una alerta cuando el archivo cambia de una versión a otra.
		5	Verificar identidad de usuario y seguimiento de ubicación; al combinar registros de DHCP, registros de VPN, registros de WLAN, eventos de inicio de sesión del controlador de dominio, puede mantener un seguimiento de auditoría para la dirección IP para el usuario y las asignaciones de ubicación geográfica a lo largo del tiempo.
		6	El motor de reglas con las siguientes características: (a) la capacidad de incluir cualquier dato en una regla, por ejemplo: rendimiento y cambio de métricas junto con registros de seguridad, (b) cálculo distribuido en memoria que involucra nodos Supervisor y Trabajador casi en tiempo real, con altas tasas de eventos, (c) la capacidad para que la regla genere una lista de observación dinámica que puede usarse recursivamente en una nueva regla para crear una jerarquía de reglas anidadas, (d) uso de objetos CMDB en la definición de reglas y (e) lenguaje unificado basado en XML para reglas e informes que facilita la conversión de un informe en una regla y viceversa.

		7	Debe poseer varios modelos UEBA basados en aprendizaje automático; son parte de la biblioteca de reglas incorporadas: (a) detectar inicios de sesión simultáneos de dos países diferentes, para identificar accesos no permitidos (b) detectar inicios de sesión simultáneos de dos ubicaciones geográficas improbables, para identificar accesos no permitidos (c) anomalía de comportamiento de inicio de sesión: inicio sesión en servidores y en momentos en que normalmente no se inicia sesión, etc., (d) detectar tráfico a dominios generados dinámicamente. Debe tener una gran cantidad de reglas de anomalías de comportamiento incorporadas que funcionen de forma inmediata pero que el usuario puede adaptar a su propio entorno. Se proporciona un marco en el que el usuario puede escribir nuevas reglas a través de la GUI, probarlas con eventos reales y luego implementarlas en el sistema.
		8	Debe proporcionar una serie de scripts de mitigación que pueden ejecutar una acción cuando ocurre un incidente. Los scripts pueden invocarse automáticamente cuando ocurre un incidente o pueden invocarse a pedido. También debe poder escribir sus propios scripts de mitigación e implementarlos en un sistema en ejecución
		9	Debe proporcionar un marco de búsqueda flexible y unificado. El usuario debe poder buscar datos basados en palabras clave o de forma estructurada utilizando atributos analizados. En el modo en tiempo real, mostrar la transmisión de datos coincidentes desde los dispositivos. En el modo histórico, se buscan eventos en la base de datos de eventos. Los nodos Supervisor y Trabajador realizan búsquedas de manera distribuida.
		10	Debe proporcionar una gran cantidad de informes incorporados (plantillas de búsqueda), según el tipo de dispositivo y la funcionalidad, como disponibilidad, rendimiento, cambio y seguridad. Capacidad de unificación de eventos y las capacidades de profundización o búsqueda de amenazas.
		11	Debe contener una amplia selección de informes de cumplimiento listos para usar: PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13, SANS Critical Control, NIST800-53, NIST800-171.
		12	Debe proporcionar una amplia variedad de paneles para que el usuario visualice los datos que recopila y los incidentes que se han desencadenado: paneles de resumen, paneles de widgets, panel de servicios comerciales, panel de incidentes, panel de identidad y ubicación.

		13	Debe poseer un sistema de tickets incorporado para administrar incidentes a través de tickets. Admitir el ciclo de vida completo del boleto de apertura, escalado, cierre, reapertura y creación de casos con archivos adjuntos para evidencia.
		14	Debe integrarse con sistemas de tickets de terceros. Cuando se produce un incidente, debe de crear un ticket en el sistema de tickets externo y vincularlo a un dispositivo existente o se puede crear un nuevo dispositivo en el sistema externo. Puede personalizar varios campos de incidentes al campo del sistema de tickets externo. Cuando el boleto se cierra en el sistema de boletaje externo, el boleto debe de cerrarse localmente.
		15	Debe de ser compatible por defecto con varios sistemas de tickets externos de terceros, por ejemplo, ServiceNow, Salesforce, ConnectWise y Remedy. Se proporciona una API para que se puedan construir otras integraciones.
		C. Funciones de descubrimiento y monitoreo	
		1	Debe admitir el descubrimiento y la supervisión de los servidores de aplicaciones tales como: Apache Tomcat, IBM WebSphere, Microsoft ASP.NET, Oracle GlassFish Server, Oracle WebLogic, Redhat JBOSS
		2	Debe admitir la autenticación de los siguientes servidores para descubrimiento y monitoreo: Servidores de Sistemas de Control de Acceso (ACS) RADIUS y TACACS+, Servidores de políticas de acceso a soluciones de identidad, (ISE), Bóveda de contraseñas de CyberArk, Configuración de CyberArk para enviar syslog en un formato específico, Autenticador de Fortinet, anillo de seguridad Juniper Networks RADIUS, Servidor Microsoft para autenticación de Internet (IAS), Protección de identidad única Vasco DigiPass
		3	Debe soportar las siguientes bases de datos para descubrimiento y monitoreo: IBM DB2 Server, Microsoft SQL Server, MySQL Server, Oracle Database Server
		4	Debe soportar los siguientes servidores de DHCP y DNS para descubrimiento y monitoreo: Infoblox DNS/DHCP, ISC BIND DNS, Linux DHCP, Microsoft DHCP (2003-2008), Microsoft DNS (2003-2008)
		5	Debe soportar el siguiente servidor de directorio para descubrimiento y monitoreo: Microsoft Active Directory
		6	Debe soportar el siguiente servidor de gestión de documentos para descubrimiento y monitoreo: Microsoft SharePoint
		7	Debe soportar el siguiente servidor de correo para descubrimiento y monitoreo: Microsoft Exchange

		8	Debe soportar los siguientes servidores web de gestión para descubrimiento y monitoreo: Cisco Application Centric Infrastructure (ACI), Fortinet FortiManager
		9	Debe soportar la siguiente aplicación de escritorio remoto para descubrimiento y monitoreo: Citrix Receiver (ICA)
		10	Debe soportar las siguientes herramientas de control de código fuente para la recopilación de registros a través de API: GitHub y GitLab
		11	Debe soportar los siguientes servidores VoIP para descubrimiento y monitoreo: Avaya Call Manager, Cisco Call Manager, Cisco Contact Center, Csico Presence Server, Cisco Tandeberg Telepresence Video Communication Server (VCS), Cisco Telepresence Multipoint Control Unit (MCU), Cico Telepresence Video Communication Server, Cisco Unity Connection, Fortinet FortiVoice
		12	Debe soportar los siguientes Servidores Web para descubrimiento y monitoreo: Apache Web Server, Microsoft IIS for Windows 2000 ando 2003, Microsoft IIS for Windows 2008, Nginx Web Server
		13	Debe soportar los siguientes servidores Blade para descubrimiento y monitoreo: Cisco UCS Server, HP BladeSystem
		14	Debe soportar las siguientes aplicaciones Cloud para monitoreo: AWS Access Key IAM Permissions and IAM Policies AWS CloudTrail API, AWS EC2, CloudWatch API, AWS RDS, Box.com, Cisco FireAMP Cloud, Google Apps Audit, Microsoft Azure Audit, Microsoft Office 365 Audit, Microsoft Cloud App Security, Microsoft Azure Advanced Threat Protection (ATP), Microsoft Windows Defender Advanced Threat Protection (ATP), Okta, Salesforce CRM Audit
		15	Debe soportar la siguiente consola de acceso de dispositivos para descubrimiento y monitoreo: Lantronix SLC Console Manager
		16	"Debe soportar las siguientes aplicaciones de antivirus y seguridad de host (HIPS) para descubrimiento y monitoreo: Bit9 Security Platform, Carbon Black, Security Platform, Cisco Security Agent (CSA), CloudPassage Halo, Crowdstrike, Digital Guardian CodeGreen DLP, ESET NOD32 Anti-Virus, FortiClient, MalwareBytes, McAfee ePolicy Orchestrator (ePO), Palo Alto Traps Endpoint Security Manager, Sophos Central, Sophos Endpoint Security and Control, Symantec Endpoint Protection, Tanium Connect, Trend Micro Interscan Web Filter, Trend Micro Intrusion Defense Firewall (IDF), Trend Micro OfficeScan"
		17	Debe soportar los siguientes dispositivos para monitoreo: APC Netbotz Environmental Monitor, APC

			UPS, Generic UPS, Liebert FPC, Liebert HVAC, Liebert UPS
		18	Debe soportar los siguientes Firewalls para descubrimiento y monitoreo: Check Point FireWall-1, Check Point Provider-1 Firewall, Check Point VSX Firewall, Cisco Adaptive Security Appliance (ASA), Dell SonicWALL Firewall, Fortinet FortiGate Firewall, Juniper Networks SSG Firewall, McAfee Firewall Enterprise (Sidewinder), Palo Alto Firewall, Sophos UTM, WatchGuard Firebox Firewall
		19	Debe soportar los siguientes balanceadores de carga y firewalls de aplicaciones para descubrimiento y monitoreo: Brocade ServerIron ADX, Citrix Netscaler Application Delivery Controller (ADC), F5 Networks Application Security Manager, F5 Networks Local Traffic Manager, F5 Networks Web Accelerator, Qualys Web Application Firewall
		20	Debe ser compatible con las siguientes aplicaciones de monitoreo de gestión de cumplimiento de red: Cisco Network Compliance Manager, PacketFence Network Access Control (NAC)
		21	Debe soportar los siguientes sistemas de protección de intrusos IPS para descubrimiento y monitoreo: AirTight Networks SpectraGuard, Cisco FireSIGHT, Cisco Intrusion Protection System, Cisco Stealthwatch, Cylance Protect Endpoint Protection, Cyphort Cortex Endpoint Protection, FireEye Malware Protection System (MPS), FortiDDoS, Fortinet FortiSandbox, IBM Internet Security Series Proventia, Juniper DDoS Secure, Juniper Networks IDP Series, McAfee IntruShield, McAfee Stonesoft IPS, Motorola AirDefense, Radware DefensePro, Snort Intrusion Protection System, Sourcefire 3D and Defense Center, TippingPoint Intrusion Protection System
		22	Debe soportar los siguientes Routers y Switches para descubrimiento y monitoreo: Alcatel TiMOS and AOS Switch, Arista Router and Switch, Brocade NetIron CER Routers, Cisco 300 Series Routers, Cisco IOS Router and Switch, Cisco Meraki Cloud Controller and Network Devices, Cisco NX-OS Router and Switch, Cisco ONS, Dell Force10 Router and Switch, Dell NSeries Switch, Dell PowerConnect Switch and Router, Foundry Networks IronWare Router and Switch, HP/3Com ComWare Switch, HP ProCurve Switch, HP Value Series (19xx) and HP 3Com (29xx) Switch, Juniper Networks JunOS Switch, Mikrotek Router, Nortel ERS and Passport Switch

		23	Debe soportar los siguientes Security Gateways para descubrimiento y monitoreo: Barracuda Networks Spam Firewall, Blue Coat Web Proxy, Cisco IronPort Mail Gateway, Cisco IronPort Web Gateway, Fortinet FortiMail, Fortinet FortiWeb, McAfee Vormetric Data Security Manager, McAfee Web Gateway, Microsoft ISA Server, Squid Web Proxy, SSH Comm Security CryptoAuditor, Websense Web Filter
		24	Debe soportar los siguientes servidores para descubrimiento y monitoreo: HP UX Server, IBM AIX Server, IBM OS400 Server, Linux Server, Microsoft Windows Server, Sun Solaris Server
		25	Debe soportar los siguientes dispositivos de almacenamiento para descubrimiento y monitoreo: Brocade SAN Switch, Dell Compellant Storage, Dell EqualLogic Storage, EMC Clarion Storage, EMC Isilon Storage, EMC VNX Storage Configuration, NetApp Filer Storage, Nimble Storage, Nutanix Storage
		26	Debe soportar detección de amenazas en ThreatConnect. Las siguientes fuentes de inteligencia de amenazas externas son soportadas: Emerging Threat, FortiGuard, FortiSandbox, Malware Domain, SANS, ThreatStream, ThreatConnect, TruSTAR, Zeus. En general cualquier fuente que provea un archivo CSV o que soporte STIC/TAXII standard.
		27	Debe soportar los siguientes servidores de virtualización para descubrimiento y monitoreo: HyperV, Hytrust CloudControl, Vmware ESX
		28	Debe soportar los siguientes VPN Gateways para descubrimiento y monitoreo: Cisco VPN 3000 Gateway, Cyxtera AppGate Software Defined Perimeter (SDP), Juniper Networks SSL VPN Gateway, Microsoft PPTP VPN Gateway, PulseSecure
		29	Debe soportar los siguientes scanners de vulnerabilidades para descubrimiento y monitoreo: AlertLogic Intrusion Detection and Prevention Systems (IPS), McAfee Foundstone Vulnerability Scanner, Nessus Vulnerability Scanner, Qualys Vulnerability Scanner, Rapid7 NeXpose Vulnerability Scanner, Rapid7 InsightVM Integration, Tenable.io
		30	Debe soportar los siguientes aceleradores de red WAN para descubrimiento y monitoreo: Servidor de aplicaciones de área amplia de Cisco, Acelerador WAN Riverbed SteelHead.
		31	"Debe soportar los siguientes dispositivos de Wireless LAN para descubrimiento y monitoreo: Redes Inalámbricas de Área Local Aruba, Redes Inalámbricas de Área Local Cisco, Puntos de Acceso inalámbrico Fortinet, Controladora de Red Inalámbrica Fortinet, Punto de acceso para redes de Área Local inalámbrica

			WiNG de Motorola, Redes Inalámbricas de Área Local Ruckus "

4.4.6

			Acceso a la Red basado en "Cero Confianza" con protección de endpoint.
		Se requiere de contar con una plataforma dentro de la solución para acceso remoto a la red basado en Cero Confianza "Zero Trust Network Access", Protección Avanzada de Endpoint, Filtrado de Contenido y Gestión de Vulnerabilidades.	
		1	Se debe incluir licenciamiento para 11,500 endpoints.
		2	Debe permitir la gestión centralizada de todos los endpoints.
		A. Funciones Generales	
		1	Debe permitir la gestión del cliente de seguridad de endpoint desde una consola central alojada en la Nube del fabricante
		2	Debe permitir la configuración de perfiles en función de estados asignados por el servidor DHCP presente en el firewall de administración centralizada del mismo fabricante;
		3	El licenciamiento debe estar basado en la cantidad de clientes registrados en la consola de gestión central del mismo fabricante
		4	Debe ser compatible con los siguientes sistemas operativos: Microsoft Windows: 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits) , 10 (32 e 64 bits), e 11 (64 bits), ; Microsoft Windows Server: 2012 o posterior; Mac OS X: v10.15, v10.14, 11+
		5	Debe tener interfaz gráfica de usuario al menos en el idioma inglés y español;
		6	Debe permitir la copia de seguridad del archivo de configuración del endpoint;
		7	El cliente de seguridad debe poder generar bitacora (logs) sobre las funcionalidades instaladas y configuradas
		8	Por lo menos los siguientes niveles de log deben estar disponibles: emergencia, alerta, crítico, error, aviso, informativo;
		9	El cliente de seguridad debe poder enviar los registros (logs) a la consola de gestión central.
		10	El cliente de seguridad debe permitir la configuración local vía XML (eXtensible Markup Language);

		11	El cliente de seguridad debe estar integrado con tecnologías de Sandboxing del mismo fabricante
		12	El cliente de seguridad debe contemplar el servicio de Sandboxing en la Nube del Fabricante
		13	Funcionalidades de Provisionamiento de Clientes
		14	El fabricante debe proveer un portal para descargar el cliente seguridad y permitir la instalación local
		15	Debe ser compatible con la instalación vía Active Directory de Microsoft
		16	La consola de gestión central debe ser capaz de instalar el cliente de seguridad en computadoras Windows asociadas a un dominio Microsoft
		17	Funcionalidades de Antivirus
		18	El cliente de seguridad debe ser capaz de inspeccionar archivos ejecutables, librerías y drivers en busca de virus
		19	El cliente de seguridad debe ser capaz de buscar actualizaciones de firmas automáticamente
		20	El cliente de seguridad debe ser capaz de enviar archivos para ser inspeccionados en sistemas de Sandboxing del mismo fabricante
		21	El cliente de seguridad debe bloquear canales de comunicación usados hackers o atacantes
		22	El cliente de seguridad debe notificar localmente cuando se detecta un virus
		23	El cliente de seguridad debe permitir que el usuario comience un escaneo bajo demanda
		24	El cliente de seguridad debe permitir que se comience escaneo de virus de forma automática regularmente
		25	El cliente de seguridad debe permitir visualizar los archivos puestos en cuarentena
		26	Debe permitir la configuración del perfil antivirus desde la consola central del mismo fabricante
		B. Funcionalidades de Filtrado de Contenido Web	
		1	Debe permitir la configuración del perfil de filtro de web desde la consola central del mismo fabricante
		2	El fabricante debe disponer de consultas en línea desde el cliente de seguridad sobre la categoría de determinada web (por ej. Interés general, tecnología, hacking, pornografía, etc.) para aplicar política de control de acceso a internet
		3	El cliente de seguridad debe admitir reglas estáticas de acceso al internet basado en expresiones regulares
		4	Para una URL determinadas las accesiones deben ser: permitir, bloquear, alertar o monitorear
		C. Funcionalidades de Firewall de Aplicación	
		1	El cliente de seguridad debe admitir perfiles de

			Control de Aplicaciones creados centralmente desde la consola de gestión del mismo fabricante
		2	El fabricante debe disponer de consultas en línea desde el cliente de seguridad sobre la categoría de determinada aplicación a modo de ser usada en la política de control de acceso
		3	Debe ser reconocido más de 2800 aplicaciones por el cliente para ser usadas en reglas de control de acceso
		D. Funcionalidades de VPN SSL	
		1	Debe permitir que el usuario cree nuevas VPN SSL
		2	Debe permitir que existan varias VPN SSL definidas simultáneamente
		3	Debe permitir la personalización del puerto TCP en el que funciona la VPN SSL
		4	Debe permitir la autenticación usando usuario y clave
		5	Debe permitir la autenticación de dos factores provisto por el mismo fabricante
		6	Debe permitir la autenticación usando certificados digitales
		E. Funcionalidades de VPN IPSec	
		1	Debe permitir que el usuario cree nuevas VPN IPSEC
		2	Debe permitir que existan varias VPN IPSEC definidas simultáneamente
		3	Debe permitir la autenticación usando usuario y clave
		4	Debe permitir la autenticación usando certificados digitales
		5	Debe permitir la selección de Modo Main y Agressive;
		6	Debe permitir la configuración de DHCP sobre IPSec;
		7	Debe permitir el uso de NAT Traversal;
		8	Debe permitir la elección de grupos Diffie-Hellman (1,2,5 e 14);
		9	Debe permitir la configuración de expiración de claves IKE;
		10	Debe permitir el uso de Perfect Forward Secrecy;
		11	Debe permitir la autenticación de dos factores provisto por el mismo fabricante
		F. Funcionalidades de Scanner de Vulnerabilidades	
		1	El cliente de seguridad debe tener integrado un módulo de búsqueda de vulnerabilidades y permitir la gestión central desde la consola del mismo fabricante
		2	Debe permitir que el usuario comience un análisis de vulnerabilidades bajo demanda

		3	Las vulnerabilidades encontradas deben ser mostradas localmente con un vínculo para visualizar información desde una base de datos en internet. Debe tener al menos: nombre, severidad y detalles
		G. Funcionalidades de Gestión	
		1	La consola de gestión centralizada deberá estar instalada en la Nube del Fabricante como un servicio de Software as a Service.
		2	Debe ser entregada sin costo adicional para la institución
		3	Debe permitir adicionar clientes mediante la adición de licencias
		4	Debe tener interfaz de gestión gráfica
		5	Debe tener la funcionalidad de backup
		6	Debe permitir la creación de usuarios de diferente perfil administrativo
		7	Debe permitir importar información desde Active Directory mediante LDAP
		8	El registro manual de estaciones debe permitir el uso de clave
		9	Debe permitir la creación de grupos de clientes para facilitar la gestión
		10	Debe permitir la configuración de clientes mediante definición XML
		11	Debe permitir la importación de configuración de perfiles desde firewall de mismo fabricante
		12	Debe permitir configuración de diferentes grupos y perfiles para facilitar la administración
		13	Debe permitir la configuración de perfiles de antivirus, webfilter, control de aplicaciones, scanner de vulnerabilidades y VPN
		14	Debe permitir habilitar la protección en tiempo real
		15	Debe permitir configurar la búsqueda de virus y vulnerabilidades de forma programada
		16	Debe permitir ejecutar escaneo total y escaneo rápido
		17	Debe permitir configurar filtro de URLs provisto por el fabricante con al menos las siguientes acciones: bloquear, advertir, permitir y monitorear;
		18	Debe permitir configurar filtro de URLs basado en wildcards o expresiones regulares con las siguientes acciones: bloquear o permitir;
		19	Debe permitir al usuario configurar VPNs localmente
		20	Debe permitir al usuario desconectar una VPN
		21	Debe permitir la conexión de VPN antes de login
		22	Debe permitir conexión automática de VPN

		23	Específico y general para VPN IPSec (al menos): - Uso de certificados o usuario y clave para autenticación - Uso de certificados en smartcard - Verificación de checksum - Bloqueo de tráfico IPv6
		24	Específico a SSL VPN (al menos): - Especificación de la IP del concentrador - Especificación del puerto del concentrador
		25	Opción para que el usuario pueda acceder a la configuración del cliente mediante contraseña
		26	Envió de logs hacia sistemas de logs externos del mismo fabricante
		27	Registro junto al sistema de gerencia de forma silenciosa (de forma que sea no perceptible para usuario);
		28	Instalación de certificado digital en el cliente
		29	Debe permitir habilitar funcionalidades de Single Sign On
		30	El sistema de gestión central debe tener disponible información sobre: Cantidad de dispositivos gestionados, Versión de Sistema Operativo, Perfil aplicado, Usuario, Versión de firmas de Antivirus
		31	Estado del cliente de seguridad: Registrado o no registrado
		32	Información sobre el sistema operativo en el que está instalado el cliente
		33	Perfil de seguridad creados y/o aplicados
		34	Funcionalidades de seguridad aplicadas: antivirus, filtro web, VPN, firewall de aplicaciones;

4.5

Módulo	Clasificación Funcional		Descripción de la Función
Dos (2) Balanceadores de aplicaciones y web application firewalls	Balanceo de aplicaciones y Firewall para aplicaciones Web	1	Los equipos deberán soportar los siguientes modos de despliegue: - Transparente. - Proxy Inverso. - One-Arm. - Router. - Direct Server Return. - Aceleración SSL por Software
		2	La solución deberá soportar al menos los siguientes interfaces: - 8 interfaces 1GE SFP. - 12 interfaces 10GE QSFP+.
		3	Throughput L4 de 60 Gbps
		4	Throughput L7 de 35 Gbps.

		5	1,200,000 Conexiones por Segundo L4.
		6	4,000,000 Peticiones HTTP por segundo L4.
		7	72,000,000 Conexiones Concurrentes L4.
		8	280,000 conexiones por Segundo L7 (1:1).
		9	40,000 conexiones por Segundo SSL (claves 2k, cifrado AES256-SHA).
		10	25 Gbps Throughput Compresión.
		11	240 GB SSD de almacenamiento.
		12	Soporte de 10 instancias virtuales.
		13	64 GB de Memoria.
		14	Soporte de integración con HSM de SafeNet.
		15	Soporte de instancias virtuales dentro del mismo equipo, pudiendo tener configuraciones y límites de rendimientos por cada una de dichas instancias.
		A. Gestión	
		1	La solución se podrá gestionar a través de los siguientes mecanismos y protocolos: - SSH. - Interfaz Gráfica a través de HTTP/S. - API RESTful. - Consola.
		2	La solución permitirá la definición de perfiles de acceso basados en roles con los siguientes permisos y opciones para cada apartado de configuración: - Escritura y lectura. - Sólo lectura. - Sin acceso.
		3	Política de contraseñas, permitiendo fijar una longitud mínima de contraseña o definir los tipos de valores permitidos.
		4	Autenticación contra repositorios externos LDAP y RADIUS.
		5	Soporte de una solución de gestión centralizada con un mecanismo sencillo de licenciamiento.
		6	No será necesario hardware adicional para la plataforma de gestión centralizada, únicamente se soportará en formato de máquina virtual.
		7	Soporte de gestión a través de API RESTful.
		8	Capacidad de la solución para programar la generación de backups cifrados por contraseña y ser almacenados automáticamente en un repositorio externo a través de SCP, TFTP o SFTP.
		9	Respaldo y Restauración de Configuraciones

		10	La solución soportará procedimientos para realizar un respaldo de la configuración del sistema, incluyendo: - Backup: generar un respaldo de la configuración actual en un fichero de texto plano. - Restore: restaurar una configuración previamente guardada en formato de texto plano. - Auto Backup: generar un respaldo de configuración automáticamente en base a la programación establecida.
		11	Almacenamiento de la configuración respaldada en el equipo local, en un servidor, o en el propio FortiADC.
		B. Alta Disponibilidad	
		1	La solución podrá operar en los siguientes modos de alta disponibilidad: - Activo-Pasivo. - Activo-Activo. - Activo-Activo-VRRP.
		2	Sincronización de configuración y de sesiones.
		3	Posibilidad de failover en tiempo inferior a 1 segundo.
		4	No será necesaria una solución de gestión centralizada para gestionar un cluster de dispositivos.
		5	Las diferentes unidades del cluster sincronizarán al menos los siguientes objetos: conjuntos de reglas, políticas configuradas y objetos.
		6	La capacidad del cluster en modo Activo-Activo incrementará el rendimiento de la solución en un 50% pudiendo soportar hasta 8 dispositivos en cluster.
		C. Routing Dinámico y Servicios	
		1	Soporte de los siguientes protocolos de routing:
		2	BGP.
		3	OSPF.
		4	Route Health Injection: permite anunciar rutas por OSPF o BGP hacia los servidores virtuales en base al estado de dicho servicio.
		D. Calidad de Servicio (QoS)	
		1	Se podrá controlar el uso de ancho de banda en base a las necesidades de la organización para mejorar la experiencia de usuario. El tráfico se clasificará en diferentes colas de prioridad con un ancho de banda asociado a cada una de ellas. Los criterios estarán basados en la tupla origen/destino/servicio
		E. Instancias Virtuales	
		1	Una instancia virtual consiste en una instancia de ADC completa que se ejecuta sobre la misma plataforma, ya sea física o virtual. Esta funcionalidad soporta despliegues multi-tenant.
		2	Se podrán políticas personalizadas para aplicar restricciones a cada instancia virtual, como por ejemplo los rangos o valores máximos para recursos:

		3	Estáticos: Servidores Virtuales, Reales, Health Checks, Grupos de Usuarios, Usuarios Locales, Páginas de Error o Pools de Origen.
		4	Dinámicos: Conexiones por segundo L4/L7/SSL, Peticiones por segundo L7, Rendimiento SSL, Sesiones Concurrentes, rendimiento entrante y saliente.
		F. Licenciamiento	
			La solución no requerirá de ningún tipo de licenciamiento para utilizar las funcionalidades de SLB, GSLB, LLB, Autenticación de Usuarios, Firewall o instancias virtuales.
		G. Balanceo de Carga Local (SLB) y Optimización de Aplicaciones	
		1	Esta funcionalidad estará disponible sin necesidad de licenciamiento adicional o de ser necesario deberá estar incluido en la oferta presentada.
		2	La plataforma de balanceo de carga ofertada deberá soportar los siguientes protocolos y aplicaciones como mínimo: - La solución deberá soportar IPv4 e IPv6. - La solución deberá soportar despliegues con IPv6 en lado cliente e IPv4 en lado servidor. - La solución deberá soportar los protocolos HTTP/1.0, HTTP/1.1 y HTTP/2. - La solución deberá soportar despliegues con HTTP/2 en lado cliente y HTTP/1.1 en lado servidor.
		3	La plataforma deberá soportar los siguientes protocolos: - HTTP. - HTTP/2. - HTTPS. - DNS. - SIP. - RTSP. - RTMP. - TCP. - TCPS. - UDP. - RADIUS. - IP. - FTP. - SMTP. - RDP. - MySQL. - MSSQL. - Diameter. - HSTS Y HPKP. - Web Socket.

		4	La plataforma deberá ser capaz de implementar comprobaciones del estado de salud de las aplicaciones y servidores para enviar el tráfico al nodo de la granja adecuado y enviar notificaciones administrativas. Cada balanceador debe tener 2 SFP+ de 10GB Multimodo, con su respectiva fibra.
		5	La plataforma deberá soportar los siguientes mecanismos de comprobación de estado de salud: - ICMP. - TCP Echo. - TCP. - HTTP. - HTTPS. - DNS. - RADIUS. - SMTP. - POP3. - IMAP4. - RADIUS Accounting. - FTP. - Oracle. - TCP Half Open Connection. - TCP SSL. - SNMP. - SSH. - L2 Detection. - UDP. - SIP. - SIP-TCP. - SNMP-Custom. - RSTP. - MySQL. - Diameter. - Script – comprobación de estado de salud avanzada a través de scripts en Shell.
		H. Balanceo de Aplicaciones, Persistencia, Reescritura/Enrutado en base a Contenidos y NAT	
		1	Soporte de los siguientes mecanismos de Balanceo: - Round Robin. - Faster Response. - Least Connection. - Destination IP Hash. - URI Hash. - Full URI Hash. - Host Hash. - Host Domain Hash. - Dynamic LB.
		2	Soporte de los siguientes mecanismos de Persistencia: - Source Address. - Source Address Hash.

			- Source Address-Port Hash. - HTTP Header Hash. - HTTP Request Hash. - Cookie Hash. - Persistent Cookie. - Passive Cookie. - Insert Cookie. - Rewrite Cookie. - Embedded Cookie. - RADIUS Attribute. - SSL Session ID. - SIP Call ID. - RDP Cookie. - ISO8583 Bitmap.
		3	Soporte de Reescritura basada en Contenido - Reescritura de cabecera HTTP y URL. - Insertar/eliminar cabecera HTTP. - Redirección en base a condición establecida. - Respuesta de 403 prohibido.
		4	Enrutamiento basado en Contenido mediante texto o expresiones regulares: - Cabecera HTTP Host. - Cabecera HTTP Referrer. - HTTP Request URL. - SNI. - IP Origen.
		5	La plataforma deberá soportar NAT: - Source NAT. - NAT. - Destination NAT. - Full NAT. - NAT46. - NAT64.
		I. Optimización de aplicaciones	
		1	La plataforma deberá soportar mecanismos de aceleración de páginas web: - Caching estático y dinámico: - Caching para respuestas HTTP con códigos de estado 200, 203, 300, 301 y 400. - Tamaño de objeto cacheado de hasta 10MB. - Tamaño de cache de hasta 500MB.
		2	Compresión/descompresión para los siguientes content-types: - application/JavaScript. - application/soap+xml. - application/x-JavaScript. - application/xml. - text/CSS. - text/html. - text/JavaScript.

			- text/plain. - text/xml. - Personalizado.
		3	Page Speed: - Optimización HTML. - Combinación de CSS, mover CSS al inicio. - Redimensionamiento de imágenes y JPEG Sampling.
		4	Multiplexación TCP: - Reutilización de conexiones TCP entre ADC y servidores de backend para optimización.
		5	Scripting - La plataforma deberá proporcionar mecanismos de scripting. - Deberá incluir Scripts predefinidos para casos de uso específicos. - Los Scripts permitirán mediante el uso de comandos predefinidos y variables, manipular peticiones y respuestas HTTP/S, SSL y TCP, así como redirecciones, persistencia, NAT, 2FA o seleccionar un enrutamiento basado en contenidos en base a las necesidades de cada entorno.
		J. Soporte SSL/TLS	
		1	Soporte de SSL Offloading, Client SSL y Server SSL para terminar el tráfico cifrado en el ADC y establecer una comunicación en claro con el backend para así reducir la carga de procesamiento en el servidor, o volver a cifrar la comunicación hacia el servidor final.
		2	Soporte de SSL Visibility, que permitirá realizar una copia de tráfico HTTPS y TCPS, una vez descifrado, hacia el interfaz destino para ser enviado a otros sistemas para su análisis o registro.
		3	SSL Forward Proxy para tráfico de cliente, donde el ADC actúa como proxy para ambos lados de la conexión. De esta forma, el certificado y clave del servidor utilizados para negociar la conexión SSL con el cliente se derivan dinámicamente del certificado presentado por el servidor real.
		4	Soporte de HSM SafeNet Luna 7.
		5	Soporte de los métodos SSL/TLS más comúnmente empleados por servidores HTTPS, incluyendo: - SNI. - Almacenamiento local de certificados. - Almacenamiento de CAs Intermedias. - Almacenamiento de CAs. - OCSP/OCSP Stapling. - CRL. - Client certificate forwarding. - SNI forwarding. - Certificados digitales con claves tipo RSA y ECDSA.

			- Alerta vía email ante caducidad de certificado, CRL y OCSP Stapling.
		6	Soporte de versiones SSLv3 y TLS 1.0, 1.1, 1.2 y 1.3.
		7	Soporte de algoritmos de curva elíptica.
		K. Objetos Dinámicos	
		1	La solución deberá soportar integración con entornos Kubernetes a través de un conector nativo mediante el cual se podrán sincronizar objetos de manera dinámica para ser utilizados como miembros de la granja de servidores reales utilizados en la publicación de los servidores virtuales.
		2	La solución deberá soportar la posibilidad de publicar de manera sencilla, un servidor virtual existente en la plataforma ADC, en una solución GSLB prestada en modo servicio del mismo fabricante.
		L. Balanceo de Carga Global (GSLB)	
		1	La plataforma de balanceo de carga global es una solución basada en DNS que permite desplegar recursos redundados en varias ubicaciones geográficas, para garantizar la continuidad de las aplicaciones y del negocio cuando una de las áreas locales sufre un pico de carga o una caída.
		2	Esta funcionalidad estará disponible sin necesidad de licenciamiento adicional.
		3	La lista de respuestas posibles ante peticiones DNS podrá ser: - Estado de salud del servidor virtual. - Persistencia. - Proximidad geográfica. - Proximidad dinámica en base a RTT, menor número de conexiones o bytes por segundo. - Weighted Round Robin.
		4	Se soportarán las siguientes funcionalidades: - Servidor DNS Remoto para configuración de DNS forwarders. - Soporte DNS64. - Límite de Respuestas para evitar que el servidor autoritativo DNS de la solución ADC pueda ser utilizado en ataques de DDoS basados en amplificación.

		5	Soporte completo de DNS incluyendo registros: - CNAME. - A/AAAA. - MX. - NS. - TXT. - SRV. - PTR. - CAA.
		M. Balanceo de Carga de Líneas (LLB)	
		1	El balanceo de líneas ofrece redundancia de enlaces y garantiza la continuidad del negocio ante la caída de una o varias de ellas. También permite hacer una distribución del tráfico entre varios operadores en base a la criticidad de cada servicio, reduciendo así el ancho de banda necesario y mejorando la experiencia de Usuario.
		2	Esta funcionalidad estará disponible sin necesidad de licenciamiento adicional.
		3	La plataforma deberá soportar los siguientes mecanismos de LLB: - Weighted Round Robin. - Menor número de conexiones. - Menor número de conexiones por segundo. - Menor ancho de banda saliente. - Menor ancho de banda entrante. - Menor ancho de banda total. - Desbordamiento en salida. - Desbordamiento en entrada. - Desbordamiento total. - Hash IP Origen.
		4	La plataforma deberá soportar los mismos health checks disponibles en el módulo de SLB.
		5	La plataforma deberá soportar los siguientes mecanismos de Persistencia: - Par Origen-Destino. - Dirección Origen-Destino. - Dirección Origen. - Dirección Destino.
		6	La plataforma deberá soportar Policy Based Routing para enrutar el tráfico en base a IP origen/destino, puerto, protocolo, prioridad de diferentes ISP y ancho de banda máximo.
		7	La plataforma deberá soportar Rutas por Proximidad con modos de funcionamiento estático y dinámico.
		8	La plataforma deberá soportar mecanismos de entrada por DNS como Round Robin, Weighted Round Robin, Proximidad y resto de funcionalidades de GSLB disponibles.
		9	La plataforma deberá soportar Multi-Homing para conectar a través de más de un enlace y establecer

			políticas de balanceo entre grupos de al menos 256 enlaces diferentes.
		10	La plataforma deberá soportar Túneles Virtuales para ofrecer conectividad site-to-site mediante encapsulación GRE para tunelizar el tráfico entre parejas de dispositivos ADC.
		N. Autenticación de Usuarios	
		1	Esta funcionalidad estará disponible sin necesidad de licenciamiento adicional.
		2	La solución deberá soportar múltiples mecanismos de autenticación de cliente: - Básica. - Formularios. - Certificado de Cliente. - SAML. - NTML.
		3	La solución deberá soportar delegación de la autenticación mediante: - Kerberos Delegation. - Kerberos Constrained Delegation
		4	La solución deberá soportar Single Sign On (SSO) - Autenticación SAML 2.0 actuando como SP. - Soporte de IdP como Shibboleth y OpenAM/OpenSSO.
		5	ADFS Proxy Authentication - La solución deberá poder configurarse como un Proxy de ADFS para facilitar este tipo de despliegues.
		6	La solución soportará mecanismos de doble factor de autenticación (2FA) para garantizar un acceso robusto a las aplicaciones, integrándose con solución de 2FA del mismo fabricante que el ADC y con Google Authenticator.
		7	La solución deberá ser capaz de publicar aplicaciones web, ofreciendo servicios de SSO hacia los servidores finales.
		8	Soporte de aplicaciones habituales en entornos empresariales como: - Microsoft ActiveSync. - Microsoft Outlook Web Access. - Microsoft SharePoint. - Microsoft Lync. - Microsoft Exchange 2010/2013/2016. - Microsoft AD FS. - Microsoft RDP.
		O. Funcionalidades de Seguridad	
		1	Protección anti-DDoS
		2	La solución deberá ofrecer funcionalidades de protección DDoS en Capa 7 para mitigar cualquier intento de disrupción del servicio.

		3	La detección en capa de aplicación deberá proteger ante: - Límite de peticiones HTTP. - Inundación de conexiones TCP. - Inundación de peticiones HTTP.
		4	La detección en capa de red deberá proteger ante: - Inundación de TCP SYN. - Fragmentación IP. - Inundación TCP Slow.
		5	Además de las acciones habituales de permitir, denegar, o bloquear temporalmente, será posible forzar una validación basada en CAPTCHA.
		6	Firewall Capa 4 - Una política de firewall permite filtrar el tráfico en base a una tupla de condiciones que incluye IP origen, IP destino y servicio. Por defecto, las políticas de firewall deberán ser stateful.
		7	La solución deberá poder ofrecer un Servicio de Prevención de Intrusiones (IPS) que proporcione defensa contra las últimas amenazas a nivel de red, con una base de datos de más de 11.000 amenazas conocidas.
		8	La solución deberá poder ofrecer un servicio de AntiVirus y AntiMalware nativo en el propio ADC, sin necesitar el envío de ficheros o ningún tipo de integración con soluciones externas. - La base de datos de AV se actualizará de manera automática. - La solución de AV deberá estar reconocida por validadores independientes externos con una alta tasa de protección y baja tasa de falsos positivos. - Permitirá restringir el tipo de ficheros que se pueden subir a una aplicación en base al tipo y tamaño del fichero. - Deberá soportar el análisis de ficheros adjuntados en correos desde dispositivos móviles a través de OWA y ActiveSync. - La solución deberá tener una integración con soluciones de Sandbox del mismo fabricante que el ADC, pudiendo generar firmas al vuelo para ser distribuidas al ADC y otras soluciones de seguridad.
		9	La solución deberá poder ofrecer un servicio de Sandbox basado en nube, o integrarse con un appliance Sandbox físico o virtual desplegad on-premise o en entorno nube, en todos siendo el Sandbox del mismo fabricante que el ADC.
		10	La solución deberá poder ofrecer un servicio de Reputación IP

		11	La solución deberá ser capaz de detectar y discriminar dos tipos de bots: - Buscadores conocidos. - Bad robots (scanners, crwalers, spiders)
		12	La solución deberá tener un cuadro de mandos para mostrar estadísticas de eventos de clientes normales y robots.
		13	La solución protegerá contra orígenes con baja reputación como Botnets, Proxies Anónimos, Scanners, Spammers, Redes Tor y servidores de Phising.
		14	La solución deberá poder ofrecer un servicio de protección basada en GeoIP. o Este servicio proporciona una base de datos que mapea las direcciones IP a países, proveedores y proxies anónimos. o La base de datos se actualizará de manera periódica. o Se podrá utilizar esta base de datos para definir la acción a tomar cuando un servidor virtual recibe una petición desde una IP catalogada.
		P. Firewall de Aplicaciones Web (WAF)	
		1	La solución deberá cumplir con el OWASP Top 10 ofreciendo protección para todas las amenazas allí recogidas, así como disponer de un wizard para su sencilla configuración.
		2	La solución deberá de incluir las siguientes funcionalidades de lógica de seguridad negativa (Firmas de Ataques):
		3	La solución deberá tener una modelo de seguridad negativo.
		4	La base de datos de firmas se actualizará automáticamente.
		5	Se podrán realizar excepciones por firma.
		6	Las excepciones se podrán crear desde el fichero de log.
		7	Las políticas por defecto deberán estar disponibles en varias clasificaciones, como Alert Only, Medium Security y High Security.
		8	Las firmas deberán estar agrupadas en diccionarios lógicos sobre los que se podrán realizar búsquedas, incluyendo al menos: - Cross Site Scripting. - SQL Injection. - Generic Attacks. - Known Exploits. - Trojans. - Information Disclosure. - Bad Robot. - Credit Card Detection.

		9	Detección de SQL/XSS Injection - Adicionalmente a las firmas de ataques, la solución deberá proporcionar mecanismos para detectar ataques de SQL/XSS Injection en base a análisis léxico.
		10	- Escáner de Vulnerabilidades Web
		11	La solución deberá tener un escáner de vulnerabilidades web integrado con al menos los siguientes tipos de firmas: o MIME Signatures. o Message Signatures. o Files Signatures. o Context Signatures. o Apps Signatures.
		12	La solución debe tener capacidades de soportar login y crawl.
		13	La solución deberá generar informes relativos al escáner de vulnerabilidades web.
		14	Protección de API
		15	La solución ofrecerá funcionalidades de protección y validación de esquemas para Webservices.
		16	La solución proporcionará detección y validación de esquema XML y SOAP para los siguientes casos de uso: o XML Format Check. o SOAP Format Check. o XML Limit Check. o WSDL Check. o XML Schema Check. o XML XSS and SQLi Protection.
		17	La solución proporcionará detección y validación de esquema JSON para los siguientes casos de uso: o JSON Format Check. o JSON Limit Check. o JSON XSS and SQLi Protection.
		18	La solución proporcionará detección y validación de esquema OpenAPI.
		19	La solución podrá actuar como un API Gateway para realizar gestión de usuarios de API, validación de claves, control de acceso, límite de peticiones y adjuntar cabeceras HTTP en las llamadas API.
		20	Características Web Anti-Defacement
		21	La solución deberá poder prevenir, detectar y restaurar desfiguraciones en la web protegida.
		22	La solución copiará contenido del servidor web a su propio disco duro y lo comparará en intervalos de tiempo configurables para ver si los ficheros han sido modificados en el servidor web.
		23	Será posible de manera opcional restaurar los ficheros modificados.

		24	Soporte de protocolos FTP y SSH para maximizar la compatibilidad con el servidor destino a monitorizar
		25	HTTP Compliance
		26	La solución deberá ofrecer mecanismos para la validación del protocolo HTTP, incluyendo los métodos permitidos, los códigos de respuesta aceptados, las propiedades de las cabeceras HTTP, longitudes máximas de peticiones, URLs, parámetros y body.
		27	Protección de datos sensitivos (Sensitive Data Protection)
		28	La solución deberá poder prevenir fugas de información, identificando información sensible de la página y aplicando medidas de protección, como el enmascaramiento de la información a proteger, así como incluir una librería de palabras ilegales y sensibles.
		29	La solución deberá poder proteger las Cookies ante ataques como Cookie Poisoning, pudiendo forzar el cifrado de las Cookies, firma, y tiempo de vida máximo.
		30	La solución deberá poder añadir cabeceras HTTP de seguridad que incluyen content-security-policy, x-xss-protection, HSTS, x-frame-options y x-content-type-options.
		31	Validación de ingresos (Input Validation)
		32	La solución permitirá validación de parámetros en base a su tamaño máximo o tipo, en base a múltiples formatos predefinidos o a expresiones regulares.
		33	La solución permitirá validar los parámetros de tipo “hidden”.
		34	La solución permitirá restringir los ficheros en base a su tamaño o tipo, soportando múltiples formatos de vídeo, imagen, texto, audio, etc).
		35	Access Protection
		36	La solución deberá poder controlar el acceso a URLs en base al patrón completo de la URL o a las extensiones de las mismas.
		37	La solución deberá poder detectar y prevenir ataques de fuerza bruta en base a parámetros como Host, URL, Códigos de Login Fallidos o límite de accesos por IP.
		38	La solución permitirá proteger ante bots, pudiendo crear excepciones en base a direcciones IP, URLs, Parámetros, Cookie o User Agent, así como excepciones en base a Buscadores conocidos.
		39	La solución tendrá la posibilidad de detectar, alertar y bloquear intentos de login utilizando usuarios y contraseñas comprometidos en base a un repositorio de credenciales robadas que se mantiene constantemente actualizado.

		Q. Monitoreo e Informes	
		1	La solución deberá tener un cuadro de mandos que muestre el uso de recursos.
		2	La solución debería tener un cuadro de mandos que muestre estadísticas del tráfico en tiempo real incluyendo información del Ancho de Banda, Conexiones, Amenazas y Sistema.
		3	La solución deberá tener un cuadro de mandos que muestre estadísticas de tráfico del servidor, amenazas y estado de los servidores de back-end.
		4	La solución deberá tener una vista gráfica que muestre la topología de los servicios desplegados.
		5	La solución deberá permitir hacer un drill-down sencillo de al menos 1 año sobre SLB: o End to End Timing. o Ancho de banda. o Conexiones Concurrentes. o Conexiones por Segundo. o Peticiones por Segundo. o SSL Offloading. o Ratio de Compresión. o Tamaño y Hits de Cache.
		6	La solución deberá ser capaz de almacenar localmente información de eventos.
		7	La solución deberá ser capaz de almacenar localmente información de seguridad.
		8	La solución deberá ser capaz de almacenar localmente información de tráfico.
		9	La solución deberá ser capaz de enviar los tipos de log anteriores a un sistema de logs centralizado del mismo fabricante que el ADC.
		10	La solución deberá ser capaz de enviar los tipos de log anteriores a un servidor Syslog externo.

		11	La información mostrada en los logs de tráfico deberá tener al menos estas categorías: o SLB Layer 4. o SLB HTTP. o SLB TCPS. o SLB RADIUS. o SLB FTP. o GLB. o SLB SIP. o SLB RDP. o SLB DNS. o SLB RTSP. o SLB SMTP. o SLB RTMP. o SLB DIAMETER. o SLB MySQL. o LLB. o SLB ISO8583. o SLB MSSQL.
		12	La información mostrada en los logs de seguridad deberá tener al menos estas categorías: o DDoS. o Geo IP Block traffic o IP Reputation. o Web application Firewall. o Antivirus. o IPS. o Firewall.
		13	La solución deberá agregar logs por día y por tipo de ataque.
		14	El log deberá mostrar tanto los valores originales codificados, como decodificados para su análisis.
		15	La solución deberá proporcionar un cuadro de mandos para analíticas de datos donde se podrá ver al menos: o SLB o Top Source IP. o Top Destination IP. o Top Browser. o Top OS . o Top Device (PC vs. Mobile). o Top Domain . o Top URL. o Top Referrer. o Top Source Country originated. o Top Session.

		16	Reportes de funcionamiento del Web Application Firewall: o Top Attack Type for All. o Top Attack Type by VS for All. o Top VS for DDoS. o Top Destination Country for DDoS. o Top VS for GEO. o Top Source for GEO. o Top Destination for GEO. o Top Source Country for GEO. o Top Destination Country for GEO. o Top Action by Source for GEO. o Top Action by Source Country for GEO. o Top Category by VS for IP Reputation. o Top Source for IP Reputation. o Top Destination for IP Reputation. o Top Source Country for IP Reputation. o Top Destination Country for IP Reputation. o Top Attack Type by VS for WAF. o Top Attack Type by Source Country for WAF. o Top Attack Type by Source for WA. o Top Attack Type by Destination Country for WAF. o Top Attack Type by Destination for WAF. o Top Platform Name by Destination for AV. o Top Platform Name by Destination Country for AV. o Top Platform Name by Source for AV. o Top Platform Name by VS for AV. o Top Reference by Destination for AV. o Top Reference by Destination Country for AV. o Top Reference by Source for AV. o Top Reference by Source Country for AV. o Top Reference by VS for AV.
		17	La solución deberá permitir la creación de informes locales, pudiendo programar su ejecución y envío por email.
		18	La solución deberá soportar integración con Splunk a través de conector nativo.
		19	La solución deberá contar con 2 interfaces de 10GE SFP+
		20	Cada Balanceador requerido debe incluir cuatro (4) tranceivers QSFP+ de 40GE, para un total de 8 transceivers

4.5.1

			Autenticación de doble factor.
		1	Licenciado para soportar al menos 2000 usuarios locales o remotos
		2	Licenciado con 2000 tokens

		3	Licenciado para permitir al menos 150 grupos de usuarios
		4	Debe ser de tipo vm y debe estar soportado en el hipervisor del instituto.
		A. Funciones Generales	
		1	Se puede entregar en una única solución o conjunto de soluciones, siempre que cumpla con todos los requisitos
		2	Licenciamiento deberá ser basado en hardware, no en recursos
		3	Admite la opción de implementar en entornos virtualizados en los siguientes proveedores de nube pública: Microsoft Azure y Amazon AWS
		4	La solución debe soportar implementación en hardware o en ambientes virtualizados, en nubes privadas o nubes públicas
		5	La solución debe soportar crecimiento adaptativo de usuarios a través de licenciamiento (en caso de opción virtualizada)
		6	La solución debe soportar implementación en las plataformas de virtualización VMware ESXi 6.0/6.5, Microsoft Hyper-V 2012 R2 / 2016 y Xen
		7	La solución debe soportar número ilimitado de vCPUs en implementación en ambientes virtualizados
		8	La solución debe soportar administración vía interfaz gráfica (GUI) por HTTP / HTTPS
		9	La solución debe soportar administración por la línea .de comandos (CLI) utilizando Telnet / SSH
		10	Permite definir perfiles de administradores para una solución, de modo que puede segmentar la responsabilidad de los administradores por tareas operativas
		11	Incluya un indicador visual centralizado de información crítica (estado de la licencia, versión de firmware, consumo de CPU / memoria / disco, número de usuarios creados y con licencia)
		12	La solución debe soportar actualización de firmware a través de la interfaz gráfica, mediante un proceso simplificado e intuitivo
		13	La solución debe soportar la personalización de mensajes de solución estándar como páginas de error, portales de autenticación, autorregistro, restablecimiento de contraseña y otros. También La solución debe soportar la inclusión, alteración y eliminación de imágenes en mensajes / páginas sin la necesidad de recursos o conectividad externa
		14	La solución debe soportar la configuración de alta disponibilidad (HA), minimizando el tiempo de inactividad
		15	La solución debe soportar implementaciones de HA como "Active-Passive" o configuraciones de

			sincronización entre dos unidades activas
		16	La solución permite la sincronización automática de configuraciones entre todos los equipos que componen la solución HA
		17	La solución debe soportar la implementación de HA sincronizando configuraciones con dispositivos en ubicaciones geográficamente separadas
		18	La solución debe soportar la opción de copia de seguridad cifrada
		19	La solución debe soportar copias de seguridad automatizadas (programadas por criterios predefinidos), no solo bajo demanda
		20	La solución debe soportar copia de seguridad completa de la configuración, incluida la base de usuarios, grupos, tokens, certificados, configuraciones de inicio de sesión único, etc. La solución también Permite la restauración de toda la configuración directamente desde la interfaz gráfica
		21	La solución debe soportar NTP (Protocolo de tiempo de red), con el objetivo de sincronización de hora / fecha
		22	La solución debe soportar ruteo estático
		23	La solución debe soportar SNMP v1, v2 e v3 permitiendo consultar MIBs propias y envío de SMNP Traps
		24	La solución debe soportar nativo SNMP Trap que indica un cambio de estado en él HA
		25	La solución debe soportar la captura de paquetes a través de la interfaz gráfica para solucionar problemas avanzados en herramientas de análisis de paquetes (por ejemplo, Wireshark)
		26	La solución debe soportar el envío de correos electrónicos actuando como su propio servidor (localhost) o integración con servidores externos para enviar mensajes a usuarios o administradores
		27	El equipo permite el envío de correos electrónicos relacionados con el restablecimiento de la contraseña, la aprobación de nuevos usuarios, el auto registro del usuario y la autenticación de segundo factor (vía token).
		28	Permita el envío de mensajes SMS a los usuarios a través de gateway SMS de terceros
		29	La solución debe soportar el registro de todos los eventos que los usuarios de su base de datos local realizan con sus cuentas, como crear un usuario, cambiar la contraseña de un usuario y cambiar la información general
		B. Funcionalidades de autenticación	
		1	La solución debe realizar la autenticación para la gestión de identidad de los usuarios de la red, siendo un punto central de control de autenticación, donde se pueden

			consolidar múltiples métodos de autenticación
		2	La solución debe soportar autenticación de dos factores (two-factor authentication)
		3	La solución debe soportar autenticación de dos factores en al menos dos tipos diferentes de tokens, el primero es físico (token) y el segundo lógico como software para dispositivos móviles
		4	La solución debe permitir la definición de un nivel de complejidad mínima para las contraseñas de todos los usuarios registrados en la base de datos local, permitiendo la definición de un número mínimo de letras minúsculas, mayúsculas, caracteres numéricos, caracteres especiales, etc.
		5	La solución debe permitir la creación de una política de bloqueo automático de usuarios después de una serie de fallas de autenticación, evitando así los ataques de fuerza bruta
		6	La solución debe soportar la creación de usuarios a nivel local, que se puede utilizar para autenticar dispositivos según sea necesario.
		7	La solución debe permitir la creación masiva de usuarios en la base de datos local mediante la importación de una lista de usuarios que se creará en archivos externos.
		8	La solución debe permitir la creación de nuevos usuarios en la base de datos local y que el administrador pueda definir una contraseña al momento de crearlos.
		9	La solución debe permitir la creación de nuevos usuarios en la base de datos local y que el equipo genere una contraseña aleatoria y la envíe automáticamente al usuario.
		10	La solución debe permitir la creación de nuevos usuarios en la base de datos local sin la definición de una contraseña, requiriendo que use el token como el único factor de autenticación
		11	Permite asociar tokens a usuarios creados localmente en la base de datos
		12	Permite a los propios usuarios registrar sus tokens e informar la pérdida de un token automáticamente, sin la necesidad de involucrar a un administrado
		13	Eliminación automática masiva de usuarios inactivos, según criterios definidos
		14	La solución permite a los usuarios locales restablecer sus contraseñas de manera segura, sin la intervención de los administradores, por correo electrónico o preguntas de seguridad en portal de autoservicio.
		15	La solución debe soportar la creación de grupos de

			usuarios, que pueden usarse para autenticar uno o varios dispositivos.
		16	Los tokens deben generar códigos con un mínimo de 6 dígitos e intervalos que no excedan los 60 segundos
		17	La solución debe soportar autenticación de dos factores por hardware dedicado (token)
		18	La solución debe soportar autenticación de dos factores por aplicación móvil (iPhone y Android)
		19	La solución debe soportar autenticación de dos factores enviando un mensaje SMS
		20	La solución debe soportar autenticación de dos factores mediante el envío de correo electrónico.
		21	La solución debe soportar sincronización de dispositivos en hardware de generación OTP (one time password)
		22	Permite sincronizar los tokens con el equipo para su correcto funcionamiento.
		23	Permite desactivar un token cuando es robado o perdido, permitiendo su reactivación posterior cuando / si se recupera
		24	Permite la disociación de un token a un usuario y asociarlo con otro usuario cuando sea necesario, permitiendo así su reutilización
		25	Permite la autenticación de doble factor en clientes Windows, incluso con la máquina fuera de línea
		26	Debe proporcionar un portal web para que los usuarios se registren automáticamente, de modo que puedan acceder, completar sus datos y enviar el registro. Después de que el usuario inicia sesión, el administrador debe ser notificado automáticamente para aprobar o denegar el registro del usuario antes de que el usuario sea activado.
		27	La solución debe funcionar como un servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticación a dispositivos compatibles con dicho protocolo
		28	La solución debe soportar la integración con el servidor RADIUS remoto
		29	La solución puede funcionar como un servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticación a dispositivos compatibles con ese protocolo
		30	La solución debe tener un servidor LDAP interno que permita su configuración jerárquica, para la correcta administración por grupos o unidades organizativas de usuarios locales.
		31	La solución debe soportar la integración con un servidor LDAP remoto (como Microsoft Active Directory)
		32	La solución debe soportar la autenticación de usuarios con credenciales de redes sociales como Facebook,

			Twitter y LinkedIn
		33	La solución debe permitir a los usuarios que no tienen una cuenta local o de redes sociales autenticarse a través de un registro rápido, que garantice una trazabilidad mínima, a través de la validación de direcciones de correo electrónico o números de teléfono.
		34	La solución debe permitir el inicio de sesión automático de los usuarios visitantes después de que se hayan registrado con éxito
		35	La solución debe permitirle configurar los parámetros de red (como la configuración de WiFi) en un dispositivo de usuario (laptop, móvil) mediante la descarga de un script o un archivo ejecutable a través del portal de visitantes.
		36	La solución debe soportar el lenguaje de marcado de aserción de seguridad (SAML), que actúa como un proveedor de identidad (IDP), estableciendo una relación de confianza para la autenticación segura de los usuarios que intentan acceder a un Proveedor de Servicios (SP)
		C. Funcionalidades de Control por Puerta	
		1	La solución debe soportar de forma nativa (sin redireccionamientos) la integración y autenticación de conmutadores y otros dispositivos compatibles con el estándar 802.1X
		2	Debe proporcionar de forma nativa (sin redirigir a equipos de terceros) la integración de los clientes finales para ofrecer autenticación 802.1X
		3	La solución debe soportar los siguientes métodos EAP 802.1X: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS y EAP-GTC
		4	La solución debe soportar la interoperabilidad con equipos de acceso de terceros (swtiches), para la autenticación de puertos con la solución, a través de los estándares 802.1X
		5	Debe ser compatible con el bypass de autenticación 802.1X para dispositivos conocidos que no son compatibles con 802.1X, el lanzamiento debe realizarse en función de la dirección MAC del equipo previamente registrado, tendrán acceso a la red sin necesidad de autenticación o acción del usuario o dispositivo.
		D. Funcionalidades de Autoridad Certificadora	
		1	La solución debe actuar como una Autoridad de Certificación (CA)
		2	Permite la administración de certificados digitales, con emisión y revocación.
		3	Permite el uso de CAs de confianza, para validar certificados emitidos por CAs externas

		4	Debe ser compatible con OCSP para proporcionar una lista de revocación de certificados (CRL)
		5	Debe proporcionar un repositorio para la autenticación VPN site-to-site a través de certificados
		6	Debe ser compatible con el servidor SCEP (Simple Certificate Enrollment Protocol), lo que permite la firma de solicitudes de certificados digitales (CSR) automáticamente o con interacción del administrador
		7	Debe crear y firmar certificados X.509 para usar en servidores https y ssh, así como clientes de servicios HTTPS, SSH, VPNs IPSec
		8	Debe poder importar otros certificados de CA, así como la lista de revocación de certificados
		9	Permite que el administrador del sistema genere, firme y revoque certificados digitales para los usuarios
		E. Funcionalidades de Single Sign-On	
		1	La solución debe proporcionar la capacidad de servicio SSO (Single Sign-On), con autenticación transparente de usuarios (pasiva) en sistemas compatibles
		2	Debe poder integrarse con un directorio activo (Windows AD) y poder ofrecer la funcionalidad SSO, donde la autenticación automática / transparente a través de SSO para los servicios necesarios se basa en la autenticación previa del usuario en el dominio
		3	Permite definir una lista de usuarios de SSO que serán ignorados, evitando así la interferencia de cuentas de servicio como antivirus o scripts a través de GPO
		4	La solución debe soportar el análisis de archivos syslog enviados desde una fuente remota, para uso del servicio SSO
		5	La solución debe soportar el Security Assertion Markup Language (SAML), para solicitar información de identidad del usuario a Proveedores de identidad (IDP) de terceros.
		6	La solución debe soportar SSO basado en radius (RSSO - RADIUS Single Sign-On)
		7	La solución debe soportar el RSSO RADIUS Accounting Proxy, que permite la recepción de paquetes de radio de búsqueda, la modificación de estos paquetes y el reenvío de ellos a varios otros puntos

4.5.2

			Detección y respuesta extendida para amenazas avanzadas en el Endpoint.
			La solución para la detección y respuesta extendida de amenazas en computadoras y servidores clave, sin necesidad de firmas, deberá incluir el licenciamiento necesario para proteger al menos 1000 dispositivos, con la solución de detección y respuesta.

		A. Funcionalidades Generales	
		1	La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows (32-bit & 64-bit versiones) XP SP2/SP3, 7, 8, 8.1 y 10
		2	La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows Server 2003 R2 SP2, 2008 R1 SP2, 2008 R2, 2012, 2012 R2, 2016 y 2019
		3	La solución propuesta debe ser compatible con los siguientes sistemas operativos: macOS Versiones: Yosemite (10.10), El Capitán (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14) y Catalina (10.15)
		4	La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: RedHat Enterprise Linux y CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 y 7.7 y Ubuntu LTS 16.04.5, 16.04.6,18.04.1 y 18.04.2 server, 64-bit
		5	La solución propuesta debe ser compatible con los siguientes sistemas operativos: Ambientes Virtual Desktop Infrastructure (VDI) en VMware Y Citrix. VMware Horizons 6 y 7, y Citrix XenDesktop 7
		6	La solución propuesta debe tener un consumo máximo de 120MB de memoria RAM
		7	La solución propuesta debe tener un consumo promedio de menos de 2% de uso de CPU
		8	La solución propuesta debe tener un consumo menor a 20MB de espacio en disco
		9	La solución propuesta debe soporta el despliegue masivo a través de herramientas como MS System Center, JAMF, y Satellite.
		10	La solución propuesta debe trabajar sin depender de firmas hash locales conocidas para la detección de archivos maliciosos
		11	La solución propuesta debe poder registrar en tiempo real información del proceso e informaciones adicionales tal como conocer el usuario asociado con los eventos
		12	La solución propuesta debe contar con la opción de establecer contraseña para desinstalar el agente en el endpoint
		13	La solución propuesta debe poder generar un instalador de Windows Preconfigurado. Esta configuración debe permitir la instalación sin requerir interacción ni configuración por parte de los usuarios
		14	El colector que será instalado en los endpoint de la solución propuesta debe poder trabajar detrás de un proxy
		B. Funcionalidades de detección de malware	
		1	La solución propuesta debe poder funcionar en modalidad "offline" fuera de línea sin que el Agente se

			encuentre conectado a la red empresarial
		2	La solución propuesta debe poder detectar cambios realizado por procesos maliciosos en el registro de las PC.
		3	La solución propuesta debe poder detectar conexiones de red desde el dispositivo.
		4	La solución propuesta debe poder detectar actividad sospechosa asociada con archivos DLL.
		5	La solución propuesta debe poder Incorpora inteligencia de amenazas en el esquema de detección.
		6	La solución propuesta debe poder incorporar las técnicas de MITRE ATT&CK en el esquema de detección
		7	La solución propuesta debe tener la capacidad para cargar indicadores de compromisos (IOC) tales como nombre de archivo y hash de archivo, etc.) para la búsqueda de amenazas en las estaciones protegidas por la solución
		8	La solución propuesta debe identificar actividad maliciosa conocida
		9	La solución propuesta debe tener la capacidad de recibir actualizaciones diarias de inteligencia
		10	La solución propuesta debe tener la capacidad de categorizar los eventos detectados en diferentes categorías (Ej.: Malicioso, Sospechoso, No concluyente, Probablemente Seguro)
		11	La solución propuesta debe tener la capacidad de convivir con otras soluciones de seguridad endpoint del tipo antivirus tradicional o de nueva generación.
		C. Funcionalidades de prevención de malware	
		1	La solución propuesta debe tener la capacidad de prevención de ejecución de archivos maliciosos
		2	La solución propuesta debe incorporar un motor de antivirus de última generación (NGAV) basado en el kernel con capacidad de "Machine Learning"
		3	La solución propuesta debe tener capacidad de controlar dispositivos USB
		4	La solución propuesta debe tener capacidad de crear excepciones a los dispositivos USB basado en el número serial de estos
		5	La solución propuesta debe poder bloquear tráfico malicioso de exfiltración de datos
		6	La solución propuesta debe poder bloquear tráfico malicioso de comunicación hacia C&C (Command & Control)
		7	La solución propuesta debe poder frenar brechas de seguridad e intentos de ransomware en tiempo real

		8	La solución propuesta debe poder evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos
		9	La solución propuesta debe permitir que las políticas en la misma sean modificadas permitiendo varios estados como: Activa, Desactivada o solo crear "logs" para las reglas de seguridad contenidas en estas
		10	La solución propuesta debe poder ser configurada en modo de simulación donde no se realicen bloqueos, pero toda actividad maliciosa es registrada
		11	La solución propuesta debe poder permitir la modificación de las reglas de detección de eventos maliciosos para que estas reglas solo almacenen un registro o estén en modo bloqueo
		12	La solución propuesta debe poder permitir la realización de escaneos periódicos de los archivos contenidos en los dispositivos con el Agente instalado
		D. Funcionalidad post-infección requerida	
		1	La solución propuesta debe permitir el bloqueo automático de un dispositivo donde se ha encontrado una actividad causada por malware
		2	La solución propuesta debe permitir el bloqueo de las actividades realizadas por parte de archivos maliciosos
		3	La solución propuesta debe tener la capacidad de creación de White List para los archivos basados en la localización de este (File Path)
		4	La solución propuesta debe tener la capacidad de creación de WhiteList/Blacklist para del tráfico de red de las aplicaciones basada en el nombre, versión y proveedor de las mismas
		5	La solución propuesta debe tener la capacidad de crear excepciones para los falsos positivos de forma manual para marcar la actividad como falso positivo y evitar que ocurran detecciones similares.
		6	La solución propuesta debe tener la capacidad de recalificar automáticamente la actividad como falso positivo y evitar que ocurran detecciones similares.
		7	La solución propuesta debe permitir la creación de excepciones de eventos basados en direcciones IP, aplicaciones y protocolos
		E. Respuesta de incidentes	
		1	La solución propuesta debe almacenar meta-data generada por los dispositivos para que la misma sea usada en investigaciones forenses
		2	La solución propuesta debe permitir la integración con plataformas SIEMs (Security Information and Event Management) a través de un syslog
		3	La solución propuesta debe tener la capacidad de obtener capturas instantáneas de memoria o "dumps"

			de memoria que permitan la realización de procesos forenses
		4	La solución propuesta debe tener la capacidad de abrir tickets en plataformas de gestión tales como ServiceNow y JIRA
		5	La solución propuesta debe permitir la integración a través de API donde el mismo tenga la capacidad de entregar información generada en un evento tales como: Dirección IP, nombre de host, usuario, fecha / hora ocurrida, actividad sospechosa, etc.) para permitir la integración vía API
		6	La solución propuesta debe tener la capacidad para terminar un proceso basado en la clasificación de este
		7	La solución propuesta debe tener la capacidad para eliminar un archivo basado en la clasificación de este
		8	La solución propuesta debe la capacidad para restaurar la configuración base basada en la clasificación de actividad predefinida
		9	La solución propuesta debe tener la capacidad para aislar dispositivos infectados de la red.
		10	La solución propuesta debe tener la capacidad para restringir el acceso del dispositivo a la red de forma automática según la clasificación de actividad detectada
		11	La solución propuesta debe obtener visibilidad completa de la cadena de ataque y cambios maliciosos
		12	La solución propuesta debe permitir la limpieza automática de los dispositivos y revertir los cambios maliciosos mientras mantiene el tiempo de disponibilidad del dispositivo
		13	La solución propuesta debe permitir la suscripción de servicios opcionales de detección y respuesta a incidentes (Ej.: Servicios gestionados de detección y respuesta)
		14	La solución propuesta debe permitir el envío de ejecutables para su análisis a un sandbox, con la finalidad de determinar si son maliciosos o inofensivos.
		15	La solución propuesta debe proporcionar múltiples mecanismos de protección, incluida como la terminación de un proceso, eliminación de un archivo malicioso, el bloqueo de una conexión de red
		F. Descubrimiento de vulnerabilidades y comunicaciones	
		1	La solución propuesta debe tener la capacidad para descubrir aplicaciones que representen riesgo al endpoint que se estén comunicando a través de la red
		2	La solución propuesta debe tener la capacidad para realizar un parche virtual, a través de la restricción de los accesos de comunicación en aquellas aplicaciones que sean vulnerables.
		3	La solución propuesta debe permitir la reducción de las superficies de ataque utilizando políticas proactivas de

			comunicación basadas en el riesgo de acuerdo a CVE y la calificación o reputación que puede tener una aplicación
		4	La solución propuesta debe tener la capacidad para prevenir la comunicación a través de la red de cualquier aplicación no autorizada
		5	La solución propuesta debe tener la capacidad para crear políticas que tengan la capacidad de prevenir la comunicación de aplicaciones de acuerdo con la versión de la aplicación instalada
		6	La solución propuesta debe poder detectar e identificar todas las aplicaciones en los dispositivos que se comunican en la red.
		7	La solución propuesta debe poder visualizar y entregar información sobre el uso de aplicaciones en red mostrando información como los IP destinos y cuales dispositivos generan tráfico
		G. Cumplimiento, Integración y Consola de Gestión.	
		1	La solución propuesta debe cumplir con los estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS)
		2	La solución propuesta debe cumplir con el estándar HIPAA
		3	La solución propuesta debe cumplir con el estándar GDPR
		4	La consola de administración de la solución propuesta debe permitir la integración con "Active Directory" para garantizar el cumplimiento de los requisitos de la política de contraseñas de la empresa.
		5	La consola de administración de la solución propuesta debe permitir el uso de autenticación de doble factor (2FA) para acceder a la misma
		6	La consola de administración de la solución propuesta debe permitir la integración con SAML para la autenticación de los usuarios a la consola de gestión
		7	La consola de administración de la solución propuesta debe permitir el uso de roles granulares para los administradores
		8	La consola de administración de la solución propuesta debe permitir la gestión para ambientes Multi-inquilinos.
		9	La consola de administración de la solución propuesta debe permitir la gestión a través de Full Restful API
		10	La solución propuesta debe poder ser gestionada completamente en nube sin requerimiento de servicios en las premisas
		11	La solución propuesta debe poder ser gestionada en una arquitectura hibrida utilizando servicios en las premisas complementadas con otras en nube.

		12	La solución propuesta debe poder ser gestionada en una arquitectura totalmente en las premisas del cliente.
		13	La solución propuesta debe permitir la integración con herramientas de control de acceso a la red, al menos del mismo fabricante.
		14	La solución propuesta debe permitir la integración con soluciones de gestión de eventos de seguridad SIEM al menos del mismo fabricante.
		15	La solución propuesta debe permitir la integración con contrafuegos o firewalls al menos del mismo fabricante.
		16	La solución propuesta debe permitir la integración con soluciones de protección contra amenazas persistentes "sandbox" al menos del mismo fabricante.
		17	La solución propuesta debe soportar la integración con el motor de información e inteligencia de amenazas del fabricante para actualización de inteligencia de malware y amenazas
		18	La consola de administración de la solución propuesta debe permitir la visualización de los eventos registrados en los dispositivos que requieran atención
		19	La consola de administración de la solución propuesta debe permitir la visualización la salud de los Agentes instalados
		20	La consola de administración de la solución propuesta debe permitir la desinstalación remota del Agente instalado en los dispositivos
		21	La consola de administración de la solución propuesta debe permitir la desactivación/activación remota del Agente instalado en los dispositivos
		22	La consola de administración de la solución propuesta debe permitir la actualización remota del Agente instalado en los dispositivos
		23	La consola de administración de la solución propuesta debe permitir la creación de reportes ejecutivo conteniendo un resumen que describe los eventos de seguridad y el estado del sistema.
		24	La consola de administración de la solución propuesta debe permitir la creación de grupos organizativos de dispositivos en los cuales cada grupo podrá tener reglas de protección independiente de los demás
		25	La consola de administración de la solución propuesta debe permitir la exportación de bitácoras locales generadas por los Agentes desde la misma consola
		26	La consola de administración de la solución propuesta debe permitir la creación de reportes de inventario sobre los Agentes desplegados conteniendo información como: Dirección IP, Nombre de Host, Sistema Operativo, Dirección MAC, Versión de Agente instalada, Estado del Agente, Ultimo día visto por la consola

		27	La consola de administración de la solución propuesta debe la visibilidad de eventos generados por los dispositivos o eventos de acuerdo con el proceso ejecutado.
		28	La consola de administración de la solución propuesta debe permitir la integración de un SMTP externo para él envió de alertas a través de correo electrónico
		29	La consola de administración de la solución propuesta debe permitir las auditorías de cambios realizados por los administradores/operadores. Estas auditorias deben poder ser además descargas en un formato CSV

4.5.3

			Orquestación de seguridad, automatización y respuesta a incidentes
		1	Se requiere la automatización de respuesta y resolución de incidentes de seguridad detectados por SIEM u otras soluciones que forman parte de la plataforma.
		2	Debe ser predecible de costear, con una métrica basada sólo en el número de usuarios, los usuarios pueden ser usuarios nombrados o concurrentes, de modo que con 1 usuario concurrente puede permitir la conexión de hasta 10 personas o más, pero no al mismo tiempo.
		3	La solución debe admitir la concesión de licencias cuando se despliegue en redes air-gapped.
		4	El licenciamiento debe ser para 4 usuarios concurrentes.
		A. Arquitectura	
		1	El sistema debe permitir guardar las credenciales, como las configuraciones de los conectores, en bóvedas externas
		2	El sistema debe permitir la externalización de la base de datos
		3	La solución debe tener su propio equilibrador de carga cuando se despliega como un clúster
		B. Funcionalidades Generales	
		1	El sistema debe proporcionar múltiples dashboards configurables que se integren con RBAC para el control de acceso por rol.
		2	El sistema debe proporcionar un mecanismo para resaltar las alertas que se acercan al SLA configurado.
		3	El cuadro de mandos debe mostrar información específica del analista, como las alertas y las tareas asignadas al analista
		4	El sistema debe calcular una estimación del retorno de la inversión y permitir que se muestre en un panel de control.

		5	Las alertas deben clasificarse por gravedad.
		6	Los analistas deben poder configurar un dashboards específico para ellos que muestre información relevante para ellos
		7	Debe ser posible importar y exportar plantillas de dashboards.
		8	Los dashboards deben actualizarse automáticamente
		9	El sistema debe proporcionar cuadros de mando centrados en las funciones, como, por ejemplo: analista de nivel 1, analista de nivel 2, gestor del SOC
		10	El sistema debe medir las métricas SOC pertinentes, como el tiempo medio de identificación, confirmación, contención, erradicación y recuperación. Debería ser posible mostrar estas métricas en un panel de control.
		11	El sistema debe proporcionar un panel de control de la salud de la integración
		12	La solución debe admitir tableros de control específicos para cada inquilino en un entorno de múltiples inquilinos.
		13	La solución debe contar con un panel de control dedicado para supervisar el estado de salud/disponibilidad de cada integración y también el estado del sistema del motor SOAR
		14	La solución debe admitir la creación de marcas en la interfaz gráfica de usuario para diferentes arrendatarios.
		15	La solución debe proporcionar un marco de desarrollo de cuadros de mando basado en HTML/JSON/JS para permitir a los usuarios crear sus widgets de cuadros de mando personalizados e importarlos a la solución SOAR
		C. Reportería	
		1	El sistema debe proporcionar informes gráficos personalizados
		2	Debe ser posible programar los informes para que se ejecuten en un momento definido por el usuario
		3	Los informes deben estar disponibles en formato PDF o CSV
		4	Debe ser posible enviar los informes programados a un destinatario de correo electrónico
		5	El acceso a la funcionalidad de los informes debe ser controlado por RBAC
		6	Debe haber un registro de auditoría que identifique la actividad de los informes, incluida la descarga de estos.
		7	Debe ser posible incluir una serie de gráficos y métricas en los informes personalizados
		D. Analítica y Alertas	
		1	Las alertas y los incidentes deben gestionarse por

			separado, cada uno en su propio módulo de interfaz de usuario
		2	El sistema debe contar con un sistema estructurado de gestión de incidentes que admita la clasificación manual y automática de las alertas, así como la gestión estructurada de los incidentes.
		3	Los campos de las alertas deben cambiarse automáticamente al tipo de ataque correspondiente
		4	El sistema debe permitir la correlación de alertas, indicadores, activos, campañas e incidentes junto con cualquier módulo personalizado cuando varios registros compartan valores de campo similares
		5	El sistema debe proporcionar un registro de auditoría específico para cada alerta. El registro de auditoría no debe ser editable por los usuarios habituales
		6	Las interfaces de gestión de alertas e incidentes deben ser personalizables para permitir una visualización flexible de la información, incluyendo la visualización de la información de la propia alerta más la información adicional devuelta por los playbooks de investigación
		7	El sistema debe proporcionar al analista acceso tanto a los datos sin procesar como a los datos analizados a través de la vista de la alerta en la interfaz gráfica de usuario.
		8	Debe ser posible definir las condiciones que deben cumplirse antes de que se ejecute un libro de jugadas, y limitar los libros de jugadas que se muestran al analista a los que son relevantes para la vista actual
		9	El sistema debe permitir al analista vincular directamente los indicadores y crear nuevos indicadores desde la alerta
		10	El usuario debe poder añadir nuevos artefactos o IOCs al finalizar la investigación
		11	El sistema debe proporcionar una funcionalidad de búsqueda global que permita al analista buscar palabras clave en todo el sistema
		12	Debe ser posible enviar las actualizaciones, notas o acciones de la investigación a una plataforma de gestión de tickets
		13	El analista debe tener la capacidad de solicitar la creación de tickets en la plataforma de emisión de tickets con la información pertinente incluida
		14	Debería ser posible enriquecer automáticamente el ticket con datos como el host, la IP, la reputación del archivo, etc.
		15	El administrador del sistema debería tener la capacidad de gestionar el campo de comentarios y los archivos adjuntos añadiendo, editando o eliminando comentarios y mensajes

		16	El ticket debe incluir metadatos como el propietario del ticket, el estado y la prioridad. Estos metadatos deben estar disponibles para su uso dentro de los playbooks
		17	Debe ser posible controlar el acceso a las funciones de gestión de casos de manera granular utilizando el control de acceso basado en roles impulsado por la GUI
		18	La escalada de los tickets debe basarse en: prioridad, riesgo, impacto o antigüedad
		19	El sistema debe permitir al analista realizar un Análisis de Causa Raíz (RCA - relacionado con la causa del robo)
		20	El sistema debe permitir al analista realizar un análisis posterior al incidente (PIA - relacionado con la gestión del incidente)
		21	La solución debe ser capaz de realizar una búsqueda de texto completa en todos los incidentes para las notas y la descripción u otras palabras clave en los incidentes
		22	El sistema debe admitir las funciones de gestión del ciclo de vida de los incidentes, incluidas las funciones para ayudar a la ingestión de datos, el enriquecimiento, la asignación, la investigación y escalación.
		23	El sistema debe soportar la asignación de tickets a las fases de Cyber Kill chain.
		24	El sistema debe soportar la asignación y el seguimiento de acuerdos de nivel de servicio multinivel flexibles en varias fases, como: Acuse de recibo SLA, Resolución SLA
		25	Debería ser posible añadir y eliminar archivos y pruebas directamente a o desde los tickets
		26	El sistema debe proporcionar una pista de auditoría detallada para ayudar a registrar la cadena de custodia de los eventos vistos y los datos recogidos
		27	El sistema debe proporcionar funciones que ayuden a la búsqueda de amenazas y al seguimiento de campañas
		28	El sistema debe permitir al analista buscar indicadores en el SIEM o en la solución de gestión de registros directamente desde la GUI de SOAR, y procesar los resultados de la consulta.
		29	Solución Debe tener la capacidad de crear módulos personalizados desde la GUI web, un módulo es un subsistema como: Alertas, Incidentes, indicadores...etc.
		30	Debe ser posible almacenar las respuestas de las consultas de registro del SIEM directamente en el ticket correspondiente

		31	La solución debe permitir la visualización de entidades vinculadas (análisis de vínculos), como las relaciones entre incidentes, alertas, indicadores, activos, usuarios y vulnerabilidades en cada una de las interfaces de usuario de estas entidades
		32	Ciertos campos deben ser visibles y/u obligatorios bajo condiciones específicas (por ejemplo: las notas de cierre deben ser visibles y obligatorias sólo cuando el estado de la alerta se establece como cerrado)
		33	La solución debe tener una función de gestión de colas personalizable que permita la asignación automática de alertas/incidentes/tareas a varios grupos de usuarios
		34	La solución debe integrarse con el marco MITRE ATTACK, proporcionando enriquecimiento de tácticas, análisis de amenazas, investigación de incidentes y sugerencias de remediación
		35	La solución debe permitir al analista editar los campos en la interfaz de usuario
		36	La solución debe permitir a los usuarios visualizar gráficamente las entidades correlacionadas y sus atributos, como la gravedad, el nombre, el ID, etc. Un código de colores debe ayudar al analista a identificar la gravedad de cada entidad.
		37	La correlación gráfica debe estar disponible para diferentes entidades como activos, vulnerabilidades, alertas e incidentes
		38	Los playbooks deben tener propiedades que permitan que ciertos playbooks se ejecuten antes que otros en la cola en función de su importancia
		39	Debe incluir una función de sala de guerra para permitir la colaboración de todos los equipos durante las crisis, la sala de guerra debe poder crearse manualmente o escalando un ticket T1 o T2
		E. Playbooks	
		1	La solución debe tener al menos 2600 playbooks, incluyendo casos de uso, muestras y relacionados con el conector
		2	El sistema debe proporcionar un registro visual de la ejecución del playbook que identifique el estado de ejecución del playbook y ayude a la resolución de problemas mediante la identificación visual de los pasos fallidos del mismo.
		3	La ejecución del playbook debe registrarse y estar fácilmente disponible para la auditoría y la solución de problemas.
		4	Los playbook deben almacenarse de forma estructurada, por ejemplo, en una estructura de carpetas o grupos.

		5	El sistema debe proporcionar un constructor de playbook gráfico y visual de arrastrar y soltar
		6	Debe ser posible realizar acciones de corrección y del sistema desde los playbook. Los ejemplos de acciones de corrección incluyen el bloqueo del usuario, la desactivación de la cuenta, etc. Ejemplos de acciones del sistema son la actualización de tickets, la asignación de tickets, la actualización de indicadores y la aprobación de la ejecución de playbooks
		7	El administrador debe tener la capacidad de exportar el playbook incluyendo todas sus versiones guardadas (similar a SVN/GIT)
		8	Debe ser posible ejecutar múltiples playbooks de forma concurrente. El sistema debe ser escalable y permitir la ejecución de un gran número de playbooks concurrentes con nodos o licencias adicionales
		9	Las herramientas de depuración deben estar disponibles de forma inmediata con la herramienta
		10	La solución debe soportar la creación de playbooks con una interfaz visual
		11	El constructor de playbooks debe soportar: - Acciones y tareas manuales 16 Puertos GE RJ45 16 Puertos GE RJ45 - Toma de decisiones y pasos de aprobación - Playbooks anidados - Condiciones lógicas y bucles - Ejecución de scripts personalizados en Python - Correos electrónicos de texto enriquecido - Solución visual de problemas del playbook - Capacidad configurable para detener o continuar en caso de error en el paso del playbook - La capacidad de marcar los playbook como activos.
		12	El sistema debe permitir que los playbook se ejecuten de diversas maneras, como, por ejemplo: ejecución manual del playbook, ejecución al crear o actualizar un registro, ejecución en un horario o cuando se solicite un punto final api específico
		13	Los playbooks deben soportar una arquitectura de etiquetas flexible que permita a los analistas etiquetar los playbooks y otros objetos del sistema con un valor de etiqueta que se pueda buscar y procesar
		14	La solución debe tener la capacidad de: - Clasificar los playbooks en los de ingestión de datos y el resto. -Activar informes a partir de los playbook - Capturar los errores de los playbooks y las razones de los fallos y permitir la reanudación de la ejecución desde el paso fallido - Programar playbooks - Establecer variables, crear, encontrar, actualizar,

			conectores, fragmentos de código, utilidades y referencias Los pasos del playbook deben tener una capacidad de bucle incorporada (tomar una lista como entrada e iterar sobre cada elemento de la misma) - Los pasos del playbook deben tener una condición incorporada para que el paso sólo se ejecute si se cumple la condición. - Añadir una salida falsa a los pasos para simular la salida de un paso incluso sin la presencia de la conectividad de red en la que se basa el paso - Capacidad de ignorar errores en cada paso para que el playbook continúe ejecutándose si la ejecución de ese paso falla - Clonar pasos en y a través de los playbooks Alinear automáticamente los pasos del playbook - Posibilidad de seleccionar varios pasos de un playbook a la vez y eliminarlos o copiarlos en el mismo playbook o en otro diferente - Debería ser posible clonar playbook existentes - Marcar los playbooks como privados o públicos
		15	El acceso a los playbooks debe ser controlado por RBAC
		16	La solución debe leer PDF y los datos pueden ser extraídos a indicadores
		17	La solución debe soportar la iniciación del playbook en la actualización o eliminación de datos
		18	El generador de playbook debe soportar el versionado de playbook o las instantáneas para permitir la reversión de un playbook a una versión anterior.
		19	La solución debe admitir la exportación de un playbook individual/exportación de un playbook vinculado
		20	La solución debe soportar el reinicio del playbook desde el paso del playbook que falló previamente
		21	La solución debe permitir al usuario ejecutar el playbook desde el editor playbooks
		22	El sistema debe contar con playbooks personalizables que permitan un manejo diferenciado de las alertas en función del tipo. Por ejemplo, el sistema debe ser configurable para manejar una alerta relacionada con el correo electrónico de manera diferente a la relacionada con la infección del punto final
		23	El paso de condición debe aceptar cualquier combinación de operadores lógicos y comparaciones de atributos sin tener que escribir código python, por ejemplo, una condición como "si ((attr1 > X) y (attr2 < Y) entonces attr1+attr2/Z) > P" y todas sus variaciones deben ser posibles desde el propio editor de pasos sin pasos adicionales

		24	La solución debe mostrar la lista de playbooks ejecutados con la posibilidad de desglosar cada uno de ellos independientemente del módulo donde se haya ejecutado el playbook
		25	Los playbooks deben ser capaces de obtener datos y aprobaciones de aplicaciones a través de correos electrónicos con la capacidad de tomar una acción específica si se produce un tiempo de espera
		26	El editor de playbooks debe permitir acciones de deshacer/rehacer para retroceder y avanzar en las modificaciones de los playbook
		F. Conectores para integración con terceros	
		1	El sistema debe contar con un mecanismo de actualización de conectores durante su vida útil que permita actualizar los conectores del proveedor entre las versiones del software.
		2	El sistema debe tener una selección de conectores suministrados y validados por el proveedor para la integración con sistemas de terceros
		3	La documentación de los conectores debe estar disponible
		4	La solución debe tener al menos 320+ conectores de integración
		5	La interfaz gráfica de usuario debe indicar que las actualizaciones de los conectores están disponibles y proporcionar el registro de cambios de cada versión
		6	Debe ser posible que los clientes desarrollen conectores personalizados. Debe estar disponible un SDK de conectores.
		7	El sistema debe proporcionar un asistente de ingestión de datos fácil de usar para configurar la ingestión de datos desde sistemas de terceros
		8	La solución tiene que permitir ejecutar acciones de remediación y recoger datos en la red segmentada a través de un agente SOAR desplegado en el segmento de red remoto, los agentes deben soportar actualizaciones automáticas
		9	El sistema debe proporcionar un indicador gráfico (Dashboard) de la salud de los conectores que indique si la conexión con el sistema de terceros es saludable sin la interacción del usuario
		10	Las acciones de los conectores deben estar sujetas a RBAC, de modo que sólo los perfiles definidos puedan utilizar las acciones definidas
		G. Indicadores de compromiso	
		1	El sistema debe incluir una base de datos de "Indicadores" dedicada que proporcione un almacén central de indicadores únicos observados

		2	El sistema debe permitir la correlación de los indicadores observados en múltiples alertas
		3	Debe ser posible importar y exportar en bloque múltiples indicadores
		4	Debe ser posible actualizar la reputación de los indicadores de forma manual o automática en función de los nuevos datos recibidos
		5	Debe ser posible asignar a los indicadores una reputación, ya sea manual o automáticamente a partir de fuentes de inteligencia de amenazas de terceros
		6	Los indicadores deben poder agruparse por Evento, Campaña, Atacante, Vector
		7	El analista debe poder vincular los indicadores a las fases de la Cyber Kill Chain
		H. Pistas de Auditoría	
		1	El sistema debe mantener un registro de auditoría de las acciones realizadas, incluida la ejecución de las acciones manuales del playbook.
		2	El registro de auditoría debe presentarse como una línea de tiempo por incidente fácil de entender que puede utilizarse para comprender las acciones tomadas contra un incidente a lo largo del tiempo.
		3	El sistema también debe mantener un registro de auditoría del sistema que registre los eventos importantes del sistema, como el inicio de sesión del usuario, las actualizaciones, las ediciones y los cambios en los componentes del sistema. El registro de auditoría del sistema debe ser granular e incluir: el tipo o categoría de registro, el usuario, la IP de origen, la hora y el detalle de la acción.
		4	El sistema debe permitir el reenvío de los registros a un servidor syslog o a una solución SIEM
		5	La solución debe incluir un módulo de cumplimiento del GDPR que ayude a las actividades del SoC a cumplir con la norma.
		I. Gestión de usuarios y RBAC	
		1	El sistema debe proporcionar un control de acceso basado en roles (RBAC) granular y flexible. El RBAC debe permitir a los administradores configurar tanto las áreas de la GUI a las que puede acceder un usuario, como los conjuntos de datos (por ejemplo, las alertas) a los que puede acceder.
		2	El RBAC y la configuración del usuario deben ser posibles a través de la GUI
		3	El RBAC debe ser granular, permitiendo a los administradores especificar los permisos de Creación, Lectura, Actualización y Eliminación hasta el nivel de las características.
		4	La solución debe soportar la autenticación de usuarios

			internos, la autenticación de usuarios externos a través de LDAP, la autenticación de 2 factores y SAML SSO
		5	Debe permitir que la granularidad del control de acceso sea a nivel de módulo, registro o campo, ("Alertas", "máquina A con IP 1.2.3.4 infectada", "1.2.3.4" son respectivamente ejemplos de módulo, registro y campo)
		J. Capacidades de Despliegue	
		1	La solución debe ser compatible con el despliegue on-premise
		2	La solución debe utilizar una arquitectura basada en dispositivos virtuales. Debe haber una imagen de dispositivo virtual suministrada por el proveedor.
		3	El sistema debe ser escalable y resistente. Debe ser posible agrupar múltiples nodos para la resiliencia o la escalabilidad.
		4	La solución debe permitir programar una copia de seguridad del estado del sistema y de los datos para poder restaurarlos en caso de desastre.
		5	La solución debe admitir la agrupación activa-activa o activa-pasiva para las necesidades de HA y equilibrio de carga
		6	La solución debe poder desplegarse en redes de tipo air-gapped.
		7	La solución debe incluir una aplicación móvil para la gestión

4.5.4

			Detección y respuesta extendida para amenazas avanzadas en la red
		Se requiere la de detección de amenazas en la red con base en inteligencia artificial y aprendizaje de máquina.	
		1	Soportar un máximo de 32 vCPU.
		2	Soportar un máximo de memoria RAM de 256 GB
		3	Soporta 2 factores para el inicio de sesión administrativa
		4	Contar con capacidad de almacenamiento de 4 TB
		5	Admite administradores remotos LDAP/RADIUS
		6	Admite RBAC para el acceso administrativo
		7	La solución debe ser compatible con el hipervisor VMware y KVM
		A. Capacidades de detección de amenazas	
		1	Capacidad para diferenciar diferentes tipos de malware y ataques
		2	Capacidades de analista virtual para descargar/ayudar a los SecOps en la prevención de brechas. Por favor, detállelo.
		3	Capacidad de rastrear el origen de la infección, por ejemplo, WannaCry

		4	Detección en menos de un segundo sin ejecutar/ejecutar archivos como el análisis de la caja de arena
		5	La solución debe ser capaz de realizar análisis de tráfico de red de alto rendimiento, con una tasa de sniffer de 10Gps y al menos 80K+ archivos por hora
		6	La solución debe ser capaz de detener el "paciente cero", es decir, la capacidad de detener la primera descarga de malware (web) desde el host, es decir, el bloqueo en línea.
		7	La solución debe tener una tasa de detección probada mediante la validación de terceros, como los paquetes de ataque de malware de los generadores de tráfico.
		8	La solución debe proporcionar la visión MITRE ATT&CK de los ataques
		9	La solución debe ser capaz de clasificar diferentes tipos de malware (por ejemplo, troyanos bancarios) y por hosts (por ejemplo, Host1 infectado con Ransomware y Downloader)
		10	La solución debe detectar el malware "sin archivos" como categoría. Se define como "sin archivos" cuando no hay archivos plantados en los hosts infectados, sino que operan puramente en el nivel de instrucciones de la memoria/CPU.
		11	La solución puede proporcionar un panorama general para el análisis de amenazas para la investigación forense
		B. Capacidades de gestión del despliegue	
		1	La solución puede desplegarse en modo sniffer sin sensores
		2	Capacidad de integración con NGFW para la cuarentena
		3	La solución puede desplegarse en un entorno "offline/airgap" (es decir, sin Internet).
		4	La solución debe ser compatible con ICAP
		5	La solución debe admitir la configuración de la lista blanca para filtrar los hosts de confianza
		6	La solución debe ser compatible con la API REST para la automatización.
		C. Requisitos de registro e información	
		1	Visualización del ataque en formato de línea de tiempo, mostrando el origen del ataque.
		2	Exportación del COI con formato STIX v2.
		D. Integraciones de seguridad	
		La solución debe tener la capacidad de integrarse con NGFW para la cuarentena/prohibición de IP, y la capacidad de poner en cuarentena dependiendo de la gravedad del evento.	

4.5.5

			Gestión de la Seguridad para el Acceso a la Nube, para protección de ambientes de Microsoft 365.
		Se requiere la protección de ambientes de ofimática basada en nube como la aplicación Microsoft 365 y otros ambientes de nube de software como servicio.	
		1	Capacidad de analizar al menos 500 cuentas de Office 365
		2	La solución debe ser de tipo SaaS
		3	Visibilidad centralizada
		4	Extiende la protección de la seguridad de la nube a las instalaciones de la empresa
		5	Simplificar el cumplimiento de muchas normas del sector, como como PCI DSS, HIPAA, SOC2 y GDPR con políticas e informes predefinidos e informes predefinidos
		6	Supervisar los comportamientos y actividades de los usuarios y gestionar los derechos de los usuarios
		7	Prevención de pérdida de datos (DLP) y herramientas de detección de amenazas
		8	Integración con Office365, Google, Yammer, Teams, Microsoft Azure, Dropbox, Google Drive, Service Now, Github.
		9	Debe integrarse con la solución actual de recolección de logs de Firewall para identificar Shadows IT dentro de la red.
		10	Integración con las siguientes aplicaciones de Microsoft: - Microsoft Teams - Microsoft OneDrive - Microsoft sharepoint - Azure Active Directory
		A. Visibilidad	
		1	Escaneo automático de datos bajo demanda- examinar el contenido existente en todas las carpetas para identificar temas de datos sensibles o políticas de seguridad.
		2	Análisis del uso de la nube - resumir visualmente las estadísticas clave de uso, incluidas las tendencias en diferentes períodos de tiempo, así como el desglose, el recuento de accesos y el uso a lo largo del tiempo.
		3	Revisión de los derechos de los usuarios- dar visibilidad a los usuarios privilegiados, a los usuarios inactivos y a los usuarios externos.
		4	Exposición de archivos - destacar los archivos más compartidos en general, así como los archivos más compartidos de cada usuario.

		B. Seguridad de datos y protección contra amenazas	
		1	Prevención de pérdida de datos en la nube- Aplicar políticas de DLP basadas en identificadores de datos, palabras clave y expresiones regulares para los datos en reposo.
		2	Detección de amenazas- Ofrecer un abundante número de políticas out-of-the-box para detectar inmediatamente las amenazas centradas en las cuentas.
		3	Detección de malware: Contar con una política de detección de malware para detectar archivos maliciosos antes de que pongan en peligro los datos confidenciales.
		4	Análisis de geolocalización: Visualizar los patrones de acceso global y analiza la actividad para identificar los intentos de acceso entre regiones poco probables, indicativos de cuentas comprometidas.
		5	Descubrimiento de Shadow IT: Ofrecer una visión general de las aplicaciones en la nube no sancionadas que se utilizan en la organización y ofrece a los usuarios la posibilidad de controlar el uso de las aplicaciones.
		6	Evaluación de la configuración: Ofrecer un gran número de políticas listas para usar para la validación automatizada de las mejores prácticas de seguridad contra su cuenta de almacenamiento en la nube.
		C. Cumplimiento	
		1	Políticas de cumplimiento predefinidas: debe tener procedimientos predefinidos diseñados para ayudar a mantener el cumplimiento de las normas ISO 27001, NIST 800-53 V4 y NIST 800-171.
		2	Debe producir informes de cumplimiento para fines de auditoría. Estos informes muestran el cumplimiento de las normas ISO 27001, NIST 800-53 V4 y NIST 800-171.

4.6

Módulo	Clasificación Funcional		Descripción de la Función
Cuatro (4) conmutadores para interconexión de la Solución de Ciberseguridad	Conmutación de paquetes en la Solución de Ciberseguridad	1	Equipo de grado Enterprise
		2	Capacidad para L2 y L3
		3	MDI/MDIX Auto-crossover
		4	Soporte de spanning tree IEEE 802.1d, IEEE 802.1w, IEEE 802.1s
		5	Soporte para medios y velocidades de transmisión según estándares IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3ab 1000Base-T y IEEE 802.3ae 10 Gigabit

			Ethernet, según aplique para los puertos requeridos en las características específicas del equipo.
		6	Puertos con auto negociación de velocidad y dúplex
		7	Soporte para Link Aggregation IEEE 802.3ad y IEEE 802.1AX
		8	Soporte de medios y velocidades de transmisión definidas en los estándares:
		9	Soporte para VLAN Tag IEEE 802.1Q
		10	Soporte para manejo de Jumbo Frames
		11	Soporte para SNMP versiones 1, 2 y 3.
		12	Soporte para sFlow
		13	Soporte para autenticación basada en estándar 802.1x (Basada en puerto y MAC), con asignación dinámica de VLAN,
		14	Administración mediante acceso por SSH, HTTPS y consola serial (En el caso de conexión a consola serial, se debe proveer cable especifico de la marca y, de ser necesario, los convertidores necesarios para conexión a equipos con puertos USB-A y USB-C, con soporte para los sistemas operativos actuales)
		15	Soporte de configuración y monitoreo mediante REST API's
		16	Soporte para DHCP-Snooping
		17	Soporte para configuración de al menos 64 rutas estáticas
		18	Soporte para implementación de ACL's
		19	Soporte para hacer Port Mirroring
		20	Soporte para QoS basado en estándar IEEE 802.1p y basado en Type of Service
		21	Soporte para SNTP
		22	Soporte para DHCP Relay
		23	Soporte para Dynamic ARP Inspection
		24	Soporte de funcionalidades de LLDP IEEE 802.1ab
		25	Soporte para MCLAG (o característica similar que permita soportar arreglos de alta disponibilidad)
		26	Soporte para descarga y carga de archivos al equipo mediante TFTP, FTP, y GUI
		27	Administración centralizada de VLANs desde un dispositivo de gestión
		28	Capacidad de aplicar políticas entre VLANs a nivel de aplicación, IP o puertos TCP/UDP desde un dispositivo de gestión
		29	Capacidad de integrarse para la gestión con dispositivos de seguridad perimetral como cortafuegos
		30	Debe soportar los siguientes modos de administración: - Stand-alone

			- Por software o appliance de gestion - Cloud management
		A. Características específicas del equipo	
		1	1 Unidad de rack, debe incluir el kit de montaje y tornillos necesarios para su instalación
		2	48 interfaces 10 GE SFP+ 6 interfaces 40 GE QSFP+ o 4 interfaces 100GE QSFP28
		3	Puerto de administración dedicada, fuera de banda o similar, de tipo RJ45
		4	Puerto de consola serial
		5	Capacidad de conmutación mínima dúplex de 1760 Gbps
		6	Procesamiento dúplex de al menos 1518 Mpps
		7	Soporte para 4000 vlans como mínimo
		8	Memoria DRAM de 8 GB como mínimo
		9	Memoria flash 128 MB
		10	Capacidad de almacenamiento de 144000 direcciones MAC
		11	Latencia < 800 nano segundos
		12	Fuente de poder redundante 100-240V AC, 50/60 Hz
		13	Cada switch debe incluir 6 QSFP+ BiDi de 40GE. Cada switch debe incluir un cable direct attach de 10 GB de 1 metro.

4.7

Módulo	Clasificación Funcional		Descripción de la Función
Dos (2) conmutadores para recepción de WAN e Internet	Conmutadores para recepción de enlaces de WAN y de Internet e integración con Firewall de Perímetro	1	Equipo de grado Enterprise
		2	Capacidad para L2 y L3
		3	MDI/MDIX Auto-crossover
		4	Soporte de spanning tree IEEE 802.1d, IEEE 802.1w, IEEE 802.1s
		5	Soporte para medios y velocidades de transmisión según estándares IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3ab 1000Base-T y IEEE 802.3ae 10 Gigabit Ethernet, según aplique para los puertos requeridos en las características específicas del equipo.
		6	Puertos con auto negociación de velocidad y dúplex
		7	Soporte para Link Aggregation IEEE 802.3ad y IEEE 802.1AX
		8	Soporte de medios y velocidades de transmisión definidas en los estándares:
		9	Soporte para VLAN Tag IEEE 802.1Q
		10	Soporte para manejo de Jumbo Frames
		11	Soporte para SNMP versiones 1, 2 y 3.
		12	Soporte para sFlow
		13	Soporte para autenticación basada en estándar 802.1x

			(Basada en puerto y MAC), con asignación dinámica de VLAN
		14	Administración mediante acceso por SSH, HTTPS y consola serial (En el caso de conexión a consola serial, se debe proveer cable especifico de la marca y, de ser necesario, los convertidores necesarios para conexión a equipos con puertos USB-A y USB-C, con soporte para los sistemas operativos actuales)
		15	Soporte de configuración y monitoreo mediante REST API's
		16	Soporte para DHCP-Snooping
		17	Soporte para configuración de al menos 64 rutas estáticas
		18	Soporte para implementación de ACL's
		19	Soporte para hacer Port Mirroring
		20	Soporte para QoS basado en estándar IEEE 802.1p y basado en Type of Service
		21	Soporte para SNTP
		22	Soporte para DHCP Relay
		23	Soporte para Dynamic ARP Inspection
		24	Soporte de funcionalidades de LLDP IEEE 802.1ab
		25	Soporte para MCLAG (o característica similar que permita soportar arreglos de alta disponibilidad)
		26	Soporte para descarga y carga de archivos al equipo mediante TFTP, FTP, y GUI
		27	Administración centralizada de VLANs desde un dispositivo de gestión
		28	Capacidad de aplicar políticas entre VLANs a nivel de aplicación, IP o puertos TCP/UDP desde un dispositivo de gestión
		29	Capacidad de integrarse para la gestión con dispositivos de seguridad perimetral como cortafuegos
		30	Debe soportar los siguientes modos de administración: - Stand-alone - Por software o appliance de gestión - Cloud management
		A. Características específicas del equipo	
		1	1 unidad de rack, debe incluir el kit de montaje y tornillos necesarios para su instalación
		2	24 interfaces RJ45
		3	4 interfaces Gigabit Ethernet SFP
		4	Puerto de administración dedicada, fuera de banda o similar, de tipo RJ45
		5	Puerto de consola serial
		6	Capacidad de conmutación mínima dúplex de 56 Gbps
		7	Procesamiento dúplex de al menos 83 Mpps
		8	Soporte para 4000 vlans como mínimo
		9	Memoria DRAM de 512 GB como mínimo
		10	Capacidad de almacenamiento de 16000 direcciones

			MAC
		11	Latencia < 2 microsegundos
		12	Fuente de poder redundante 100-240V AC, 50/60 Hz
		13	Cada switch debe incluir 4 SFP de 1 GE

4.8

Módulo	Clasificación Funcional		Descripción de la Función
Servicios de soporte técnico y garantía de hardware y software.	Soporte técnico y garantía de hardware y software.	1	La Solución de ciberseguridad y todos sus componentes deberán incluir soporte y garantía de fábrica 7x24x365 por un plazo de tres (3) años contados a partir de la fecha de emisión del acta de recepción.
		2	El soporte y la garantía deberán de cubrir tanto a los equipos físicos como dispositivos virtuales y el licenciamiento de software necesario para el funcionamiento descrito para cada plataforma sin importar si se trata de un licenciamiento perpetuo o por suscripción.
		3	Si los equipos propuestos requieren acceso a los motores de inteligencia contra amenazas del fabricante, el servicio de soporte y garantía se debe incluir el licenciamiento o la suscripción necesaria para dichos servicios de tal manera que se posea el acceso a estas bases de conocimientos por al menos tres (3) años contados a partir de la fecha de emisión del acta de recepción.
		4	El centro de atención de llamadas de soporte o garantía deberá operar bajo el formato de tiempo 7x24x365.
		5	La atención a los incidentes por parte del fabricante deberá ser por medio de correo electrónico, llamada telefónica o chat.
		6	El servicio de soporte y garantía debe incluir el reemplazo de partes en caso de una falla.
		7	El servicio debe incluir acceso irrestricto a la documentación del fabricante, así como a la base de conocimientos de problemas conocidos.
		A. Características avanzadas del servicio	
		1	El servicio de soporte y garantía deberá estar basado en la cuenta del cliente como un todo y no dispositivo por dispositivo.
		2	El servicio deberá incluir la designación de un especialista del fabricante con funciones de gerente técnico de la cuenta, para gestionar todos los procesos relacionados con el soporte y la garantía.
		3	El servicio deberá considerar que el tiempo de respuesta a los incidentes debe ser priorizado de una forma acelerada en referencia a los clientes que no cuentan con soporte avanzado. Esto implica que el

			equipo de soporte avanzado del fabricante deberá tener un tiempo de respuesta máximo de 15 minutos para incidentes de criticidad 1 con retroalimentación de la solución al menos cada dos (2) horas y criticidad 2 con retroalimentación de la resolución al menos cada 4 horas. Todo el manejo de la información relativa a un incidente deberá ser administrada por parte del gerente técnico designado para atención personalizada al cliente.
		4	El servicio debe incluir sesiones técnicas dirigidas por el gerente técnico designado para revisar la gestión de los incidentes y recomendar mejoras identificadas de forma proactiva.
		5	El servicio debe incluir análisis de causa raíz para incidentes de criticidad 1.
		6	El servicio debe incluir entrenamiento y exámenes de certificación por parte del fabricante al menos para los dos primeros niveles iniciales existentes en la red curricular del programa de entrenamiento del fabricante para 4 personas por año por cada nivel de certificación.
		7	El servicio deberá incluir horas a demanda de atención que pueden canjearse por atención directa del fabricante en eventos críticos de configuración, cambios, fallas, etc. Deberán incluirse al menos 16 horas de apoyo por año para este tipo de tareas.
		8	El servicio por ofrecer deberá considerar que el INSTITUTO pueda designar al menos 5 contactos para poder gestionar la comunicación con el gerente técnico designado por el fabricante.
Servicio de soporte técnico	Servicio de soporte de incidentes y nuevas configuraciones	1	El OFERENTE deberá incluir el servicio de soporte con una disponibilidad de 24x7x365, para todos los componente incluidos en el presente documento, incluyendo soporte a incidentes, configuraciones nuevas y reconfiguraciones de los componentes después de implementados, designando un ingeniero VIP, el cual deberá llevar el historial y administración de dicho soporte, manejando en conjunto con el equipo de tecnología del INSTITUTO la gestión de cambios.

4.9

Módulo	Clasificación Funcional		Descripción de la Función
Servicio de implementación de la Solución de ciberseguridad	Servicio de instalación, configuración e integración de la Solución de ciberseguridad	1	El oferente debe considerar que la Solución de ciberseguridad deberá quedar completamente funcional, protegiendo la infraestructura del Instituto. Esto implica que al menos deben considerarse las siguientes etapas: - Planeación

			- Diseño - Implementación - Pruebas (HA, Failover, Conectividad, funcionamiento de las herramientas de seguridad). - Documentación
		2	El proyecto debe estar gestionado al menos por una persona con el rol de Project Manager por parte del oferente para manejo efectivo de la comunicación y coordinación con el equipo de trabajo del lado del Instituto. El Project Manager debe estar certificado por PMI o por SCRUM y deberá contar con al menos 2 años de experiencia en la gestión de proyectos de tecnología.
		3	Para el despliegue de la Solución se deben incluir al menos cinco (5) especialistas, parte del equipo local y/o regional del OFERENTE, certificados por el fabricante como expertos en seguridad de redes nivel "Profesional" enfocado en servicios de ingeniería postventa, no se aceptan certificaciones de ventas o preventas.
		4	Para el despliegue de la Solución se debe incluir al menos tres (3) especialistas, parte del equipo local y/o regional del OFERENTE, certificados por el fabricante como expertos en seguridad de redes nivel "Arquitectura" enfocado en servicios de postventa, no se aceptan certificaciones de ventas o preventas.
		5	El servicio de implementación debe incluir al menos las siguientes etapas
			Planeación:
		6	Reunión inicial del proyecto (Kick-off) para la presentación del equipo de trabajo asignado y definición de cronograma.
		7	Dimensionamientos previos a los sitios de instalación para definición de asignación de recursos físicos y materiales necesarios para la instalación de los equipos.
		8	Elaboración de la planeación para la instalación y configuración de toda la solución de este RFP
		9	Reuniones presenciales de seguimiento del proyecto, en las que se definirá el avance del proyecto y se informara si existirán cambios al cronograma indicando el responsable asociado
			Diseño:
		10	Levantamiento de información de las configuraciones actuales de los equipos y de la topología de la red para:
		11	Elaboración del diseño de segmentación lógica de la

			solución de CyberSecurity
		12	Elaboración de documentos de ingeniería
			Actividades de Implementación:
		13	Instalación física de todos los equipos contemplados en este proceso de licitación en los espacios indicados por el cliente
		14	Configuración de toda la solución contemplada en este proceso con base a las políticas indicadas por el cliente
		15	Pruebas locales de conectividad y funcionalidad de la solución.
		16	Limpieza final de lugar.
		17	Documentación de Cierre del proyecto
		A. Consideraciones especiales en la prestación del servicio	
		1	El proyecto debe incluir todos los accesorios necesarios para la correcta instalación de los componentes que forman parte de la Solución, entre ellos, pero no limitándose a los aquí nombrados: rieles de montaje en rack, cables de poder, cables de red certificados y fibras ópticas certificadas, tranceivers necesarios, organizadores de cableado horizontales y verticales de ser necesarios, y cualquier otro elemento necesario para la instalación completa de la Solución de ciberseguridad. Lo anterior implica que el proyecto debe ser manejado bajo el concepto "Llave en mano", por lo que ninguno de los accesorios necesarios para la correcta instalación de la Solución será provisto por el Instituto.
		2	Por la magnitud del proyecto es necesario que la oferta incluya al menos diez (10) días hábiles de servicios profesionales de un ingeniero o ingenieros proporcionados directamente por el fabricante en modalidad hibrida (remota, presencial) en horario laboral de 8 a.m. a 5 p.m. , dejando a discreción del OFERENTE las actividades a realizar presenciales o de manera remota, las actividades serán específicas y acotadas para configuraciones especiales de despliegue, instalación y configuración de la Solución de ciberseguridad.

		3	Por la magnitud del proyecto es necesario que la oferta incluya al menos 7 ventanas nocturnas de servicios de un técnico o técnicos proporcionados directamente por el fabricante en modalidad hibrida (remota, presencial) en horario nocturno, dejando a discreción del oferente las actividades a realizar presenciales o de manera remota, las actividades serán específicas y acotadas para momentos específicos en la migración, dejando a discreción del oferente cuando utilizarlas.
		4	El oferente deberá incluir los servicios de un especialista dedicado para apoyar al personal del Departamento de Telecomunicaciones, Conectividad y Seguridad, de la Dirección de Tecnología y Servicio del Instituto al menos por un plazo de tres (3) años. El especialista podrá ser empleado del oferente siempre que pueda estar dedicado para atender los requerimientos del Instituto.

4.10

Requerimiento de hardware para virtualización de componentes de integración de la Solución.
La capacidad necesaria de cómputo, memoria, disco, interfaces de red y virtualización necesarias para ejecutar la Solución deberán ser incluidas bajo el concepto de llave en mano, de acuerdo con las magnitudes siguientes:

Componente	vCPU	Memoria RAM	Capacidad de Almacenamiento tipo NAS CON 10,000 IOPS	Interfaces de red dedicadas
Para solución de detección y respuesta extendida para amenazas avanzadas en la red	32	128 GB	4 TB	2 x 10 Gb
Para solución de control de acceso a la red	20	32 GB	100 GB	2 x GE tipo RJ45
Para solución de orquestación de seguridad, automatización y respuesta a incidentes	8	32 GB	1 TB	1 GE tipo RJ45
Para Monitoreo de la Solución	16	64	16 TB	1 x GE RJ45 o 10 GE
Para solución de autenticación de doble factor	2	8	1 TB	1 GE tipo RJ45
Para solución de protección basada en señuelos para bloqueo de amenazas internas y externas	8	24	500 GB	1 GE tipo RJ45

Para la gestión de la Solución	6	16	1 TB	1 GE tipo RJ45
Para solución de Gestión de Eventos e Incidentes de Seguridad – SIEM	112	104	72 TB	

5. DISPOSICIONES ESPECIALES

a) Experiencia: Contar con un mínimo de cinco (5) años de experiencia en la venta, implementación y soporte de soluciones iguales o similares en Guatemala y/o la región de Latinoamérica. Para cumplir con este requerimiento deberá presentar por lo menos 3 cartas de referencia que comprueben el tiempo que se está requiriendo.

b) Ubicación geográfica: el OFERENTE deberá contar con oficinas locales en el territorio de Guatemala, y debe contar con al menos un centro de soporte regional, fuera del territorio nacional, para garantizar la continuidad de servicio en caso de problemas en territorio nacional.

c) El OFERENTE deberá indicar expresamente en su oferta el tiempo de entrega e implementación de lo requerido.

d) El OFERENTE deberá presentar carta en original o fotocopia legible legalizada que demuestre que es proveedor con el máximo nivel de certificación autorizado por parte del fabricante de la solución Ofertada a nivel local como regional.

e) El OFERENTE deberá cumplir con cada una de las siguientes Certificaciones:
-ISO 27001:2005 en sistemas de Seguridad de la información
-ISO 9001:2008
-ISO 22301-2012

f) El OFERENTE deberá presentar descripción y certificaciones del Project Manager, especialistas y técnicos establecidos en las especificaciones técnicas.

g) El OFERENTE deberá presentar la matriz de escalamiento según nivel de servicios establecidos en las Especificaciones Técnicas.

h) El OFERENTE deberá incluir dentro de su propuesta, el traslado de conocimiento de la implementación y puesta en producción de la Solución de acuerdo con lo indicado en las especificaciones técnicas del componente de capacitación.

i) El OFERENTE deberá adjuntar declaración jurada contenida en Acta Notarial en la cual garantice que la solución ofertada cumplen las ESPECIFICACIONES TÉCNICAS requeridas.

j) El OFERENTE deberá presentar en la oferta todo lo requerido, no se aceptarán ofertas parciales.

k) El OFERENTE debe presentar toda la documentación en español. Si acompaña documentación en otro idioma, deberá adjuntar su respectiva traducción. Se exceptúa manuales o documentación técnica.

l) El OFERENTE deberá mantener el acompañamiento en la ejecución y en el caso de requerirse una actualización del licenciamiento de nuevas versiones y soporte en línea, deberá proporcionarlo durante el período de la vigencia de la garantía.

m) El OFERENTE acepta desde el momento de presentar su oferta, todas las condiciones indicadas en el presente documento.

n) **Visita técnica:** Deberán realizar visita técnica en la Subgerencia de Tecnología, ubicada en la 7ª. Ave. 22-72 zona 1, Centro Cívico Guatemala, tercer nivel, Oficinas Centrales del IGSS, con la finalidad de evaluar el ambiente operativo donde deberá ser instalada la Solución de ciberseguridad integrada a ofertar al INSTITUTO. Al finalizar se entregará constancia de haber efectuado la visita técnica y detalles de las capacidades de cómputo que se requieran para soportar la Solución en sus componentes virtuales, tales como redundancia y tolerancia ante fallas.

o) Recurso Humano: El OFERENTE deberá adjuntar a su oferta el listado del personal nacional o extranjero que realizará la implementación, configuración y puesta en marcha de la solución ofertada; para su verificación deberá adjuntar los currículums y certificaciones que avalen el conocimiento necesario de cada persona que participará en el proceso.

   o.1) En el caso de ser personal profesional extranjero, estos deberán acompañar, en original o fotocopia legible legalizada, del diploma o título de la institución que lo acredite.

p) La AUTORIDAD ADMINISTRATIVA SUPERIOR nombrará una Comisión Receptora conformada por tres (3) técnicos con conocimientos en la materia propuestos por la Subgerencia de Tecnología. LA COMISIÓN RECEPTORA tiene la responsabilidad de suscribir un Acta de Recepción en la cual se haga constar que se recibe de conformidad con lo establecido en las ESPECIFICACIONES TECNICAS y DISPOSICIONES ESPECIALES, contemplando lo siguiente:

   p.1) Verificar que la Solución integrada de Ciberseguridad sea entregada bajo la modalidad "LLAVE EN MANO", garantizando la compatibilidad, integración, interoperabilidad y funcionalidad del OBJETO de este evento.

   p.2) Verificar que el licenciamiento propuesto por el CONTRATISTA corresponda al entregado.

q) La Subgerencia de Tecnología podrá designar a un Técnico Supervisor, quien será el responsable de verificar que los equipos sean funcionales en el momento que sean encendidos y tendrá la facultad de requerir toda aquella información que considere pertinente durante este proceso a todos los involucrados para resolver o solventar dudas.

r) La solución integrada de ciberseguridad ofertada, deberán ser entregada bajo la modalidad "LLAVE EN MANO", garantizándose compatibilidad, integración, interoperabilidad y funcionalidad entre los está la infraestructura tecnológica con la que cuenta el INSTITUTO, es decir, que todos los elementos necesarios para que la solución ofertada funcione correctamente, deberán incluirse.

s) La capacidad necesaria de cómputo, memoria, disco, interfaces de red y virtualización necesarias para ejecutar la Solución deberán ser incluidas bajo el concepto de llave en mano.

t) Los daños físicos o pérdidas derivadas del transporte, instalación, configuración y puesta en funcionamiento de la solución, así como sus respectivos componentes y accesorios, deberán ser asumidos por el CONTRATISTA, lo cual no incurrirá en gastos adicionales para el INSTITUTO.

u) El tiempo de entrega no podrá ser mayor de **ciento ochenta (180) días calendario**, contados a partir de la notificación de la resolución de aprobación del CONTRATO.

v) El OFERENTE deberá proveer fotocopia simple del cuadrante de Gartner en donde aparezca la marca ofertada.

5.1. INSTALACIÓN

a) Durante las diferentes fases del proyecto será necesario que la metodología de gestión de proyectos a utilizar brinde los siguientes documentos como mínimo:

1. Etapa de iniciación
    - Acta constitutiva del proyecto
    - Minuta de reunión de kick-off
2. Etapa de planificación:
    - Matriz de riesgos
    - Plan de proyecto
3. Etapa de ejecución:
    - Acta de aceptación
    - Acta de entrega de solución

4. Etapa de cierre:

    - Acta de cierre de proyecto
    - Encuestas de proyecto
    - Informe de cierre de proyecto

5. Etapa de seguimiento y control
    - Informe mensual de avance de proyecto

b) EL CONTRATISTA deberá entregar, instalar y configurar dejando operativos todos los componentes que forman parte de la Solución, en el Centro de Datos de la Subgerencia de Tecnología, ubicado en el tercer nivel, Oficinas Centrales, 7ª Avenida 22-72 Zona 1, Centro Cívico.

c) EL CONTRATISTA, sus subalternos y demás personal con relación de dependencia no podrán revelar información confidencial propiedad del INSTITUTO sin el previo consentimiento por escrito de este último, asimismo, no permitirá la divulgación escrita o verbal de datos y de la información que tenga acceso derivado la instalación, configuración y puesta en producción de la Solución, ni suministrará a terceros, información relacionada con el secreto profesional.

d) La implementación deberá ser realizada por técnicos certificados en la solución ofertada de acuerdo con las especificaciones técnicas.

e) Todos los equipos deberán ser instalados e implementados en el centro de datos del Instituto.

f) Al finalizar el proceso de implementación, toda la instalación y configuración realizada, deberá quedar debidamente documentada y entregada al Departamento de Infraestructura Tecnológica de la Dirección de Tecnología y Servicio del Instituto.

5.2 CAPACITACIÓN

Módulo	Clasificación Funcional		Descripción de la Función
Capacitación con certificación en las soluciones ofertadas.	Capacitación general para todos los componentes de la Solución integrada de ciberseguridad, incluyendo derecho a examen de certificación	1	Se deberá incluir el acceso a los cursos y sus respectivos laboratorios de manera online para todas las soluciones ofertadas, por un plazo de seis meses a partir de la notificación de aprobación del contrato. Una vez que se haga el enrolamiento de los técnicos o especialistas del Instituto en estos laboratorios, deberán permanecer activos, para realizar las practicas y configuraciones de los laboratorios requeridos por el curso.
		2	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de firewall.
		3	Se debe proveer acceso a laboratorio para tener una

			parte práctica a nivel de la solución a realizar upgrade de la parte de analítica, con la que ya cuenta el Instituto.
		4	Se debe proveer acceso a los laboratorios para contar con retroalimentación en parte práctica de la solución para realizar actualizaciones en gestión de los firewalls con los que ya cuenta el Instituto.
		5	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de la solución de seguridad de endpoint
		6	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de la solución de EDR.
		7	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de la solución balanceo de carga.
		8	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de la solución de doble factor de autenticación.
		9	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de la solución de NAC
		10	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de administración de diseño e implementación de la solución SOAR.
		11	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de administración de la solución de SOAR
		12	Se debe proveer acceso a laboratorio para tener una parte práctica a nivel de la solución de Firewall a nivel avanzado.
		13	Se debe proveer acceso a laboratorio a nivel de protección avanzada de amenazas. Con la finalidad de mejorar el análisis que realizara el personal del instituto.
		A. Certificación	
		1	Con la finalidad de entregar valor al Instituto y al personal, se solicita que se incluyan los exámenes necesarios de certificación para las siguientes tecnologías:
		2	Voucher de certificación para 4 personas para la solución de Firewall.
		3	Voucher de certificación para 4 personas para la solución de NAC.
		4	Voucher de certificación para 4 personas para la solución de balanceo de carga.

		5	Voucher de certificación para 4 personas para la solución de SIEM.
		6	Voucher de certificación para 4 personas para la solución de SOAR.
		7	Voucher de certificación para 4 personas para la solución de EDR.
		8	Voucher de certificación para 4 personas para la solución de switch.
		9	Voucher de certificación para 4 personas para la protección avanzada contra amenazas.
		10	El derecho para tomar cada uno de los exámenes deberá estar disponible al menos por un plazo de 6 meses, a partir de la notificación de aprobación del contrato.

5.3 GARANTÍA DE FABRICACIÓN

La garantía debe incluir lo siguiente:

a) Se requiere que la garantía de fábrica, en adelante "**la garantía**", tenga cobertura durante un periodo de **tres (3) años en sitio,** contados a partir de la fecha de emisión del acta de recepción, para los equipos y licenciamiento ofertados, para lo cual el OFERENTE deberá incluir en su OFERTA, declaración jurada contenida en Acta Notarial con la descripción completa de los alcances, beneficios y limitaciones de la garantía ofrecida, para la solución ofertada.

b) Acceso remoto a un administrador de servicios de tecnología provisto por la fábrica; con las siguientes responsabilidades:

- Envío de reporte mensual de los casos de soporte abiertos y cerrados.
- Verificación de las versiones actualmente instaladas en el ambiente y comparación con las recomendaciones de fábrica.
- Revisión del estado de contratos de soporte, fechas de inicio, vencimiento y detalles de este.
- Asistencia durante la atención a casos de soporte, coordinación de recursos para la atención de casos, y escalación prioritaria ante eventos de severidad uno (1).

c) La relación para el cumplimiento de la garantía será directamente entre el CONTRATISTA y el INSTITUTO. Todas las características del servicio de garantías ofrecidas se deberán encontrar operativas en la República de Guatemala.

d) Si se determina que los equipos recibidos por el INSTITUTO tienen fallas de fábrica, el CONTRATISTA deberá reemplazarlos por otros nuevos e iguales características a los ofertados sin costo alguno para el INSTITUTO, en un plazo máximo de treinta (30) días

hábiles; contados a partir de la fecha de presentación del reclamo, e instalarlos, configurarlos y dejarlos en operación, en el lugar de destino final.

e) Todos los equipos deberán ser nuevos, sin uso y en perfecto estado de funcionamiento.

f) El software propuesto por el CONTRATISTA deberá incluir el derecho de actualización de nuevas versiones y soporte en línea durante el tiempo que dure la garantía.

5.4 SOPORTE TÉCNICO LOCAL, SEGUIMIENTO Y SOLUCIÓN DE CASOS:

Para los casos que son clasificados por el Instituto Guatemalteco de Seguridad Social como:

1. **Prioridad Crítica**: El CONTRATISTA se compromete a atender la consulta en un plazo máximo de quince (15) minutos. Con todos los medios técnicos a su alcance, recomendará telefónicamente una solución o alternativa de solución en un tiempo de dos (2) horas.

2. **Prioridad Grave**: El CONTRATISTA se compromete a atender la consulta en un plazo máximo de quince (15) minutos. Con todos los medios técnicos a su alcance, recomendará telefónicamente una solución o alternativa de solución en un tiempo de cuatro (4) horas.

3. **Prioridad Importante**: El CONTRATISTA se compromete a dar una solución o alternativa de solución en un plazo máximo de veinticuatro (24) horas.

4. **Prioridad Baja:** El CONTRATISTA se compromete a buscar la información y enviarla al INSTITUTO en el momento en que la misma esté disponible.

5. El soporte técnico deberá ser 7x24x365 durante el período de vigencia de la garantía. El servicio podrá iniciar con una llamada telefónica o una conferencia remota y puede finalizar con la visita presencial para lograr resolver el problema planteado y el Instituto Guatemalteco de Seguridad Social acepte formalmente la solución.

6. El OFERENTE deberá adjuntar a su oferta una (1) carta en original o fotocopia legible legalizada por medio de la cual certifique que posee la infraestructura necesaria local y/o regional para cubrir requerimientos de garantía de los equipos que forman parte de la solución. Entre ellos e indispensables:

    a) NOC 24x7x365 a disponibilidad por la duración del proyecto.
    b) CSOC 24x7x365 a disponibilidad por la duración del proyecto.

5.5 GARANTÍA DE CALIDAD Y/O FUNCIONAMIENTO

El INSTITUTO hará efectivo el cumplimiento de la garantía por las siguientes causas:

a) Cuando el CONTRATISTA incumpla cualesquiera de las condiciones establecidas en: ESPECIFICACIONES GENERALES, ESPECIFICACIÓN TECNICAS Y DISPOSICIONES ESPECIALES.

b) Cuando los EQUIPOS que conformen la solución integrada de ciberseguridad entregados no correspondan a los cotizados y adjudicados.

c) Cuando restituyan los EQUIPOS defectuosos o dañados y nuevamente estén defectuosos.

d) Cuando la solución propuesta no permita un crecimiento a lo establecido en el objeto adjudicado.

5.6 FORMA DE PAGO

El INSTITUTO pagará el OBJETO de la adquisición que fue requerido por la UNIDAD SOLICITANTE recibido y a entera satisfacción, en dos (2) pagos, así: Primer pago de 85% del monto total, luego de la entrega de la Solución Integrada de Ciberseguridad; Segundo pago de 15% al finalizar la configuración, implementación, capacitación y puesta en funcionamiento de la solución; dentro del plazo de treinta (30) días posteriores a la fecha de presentación de la Factura Electrónica FEL y demás documentación que se le requiera, por medio de depósito en cuenta monetaria del Banco de Desarrollo Rural, Sociedad Anónima, -BANRURAL- u otros del sistema que el CONTRATISTA haya registrado.

El trámite de dicho pago estará a cargo de la UNIDAD SOLICITANTE, quien procederá de conformidad con la normativa del INSTITUTO. En caso que, el OBJETO no sea pagado en el ejercicio fiscal vigente, se afectará la partida presupuestaria autorizada para el ejercicio fiscal siguiente, por el órgano director del INSTITUTO y que corresponda a la UNIDAD SOLICITANTE. (Artículo 62 de la LEY).

6. ANEXOS

6.1 Instructivo para el llenado de los Requisitos de las Bases en el FORMULARIO ELECTRÓNICO.
6.2 Formulario de Identificación del OFERENTE.
6.3 Cuadro de ESPECIFICACIONES TÉCNICAS REQUERIDAS del EQUIPO
6.4 Listado del personal propuesto para la implementación, configuración y puesta en funcionamiento del EQUIPO.
6.5 Constancia de Visita.
6.6 GLOSARIO
FORMULARIO ELECTRÓNICO.
Proyecto de CONTRATO.

6.1 INSTRUCTIVO PARA EL LLENADO DE LOS REQUISITOS DE LAS BASES EN EL FORMULARIO ELECTRÓNICO

DOCUMENTOS DE LICITACIÓN DA No. 687-IGSS-2023

ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD, REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-.

El OFERENTE deberá ingresar los datos solicitados en los Requisitos de las Bases en el FORMULARIO ELECTRÓNICO en GUATECOMPRAS, tomando en cuenta los siguientes parámetros, la JUNTA deberá verificar su cumplimiento.

DOCUMENTO		**PARÁMETROS QUE DEBERÁ INGRESAR EN EL FORMULARIO ELECTRÓNICO**
a)	FORMULARIO ELECTRÓNICO.	1. Formulario Electrónico.
b)	Original del Seguro de Caución de Sostenimiento de Oferta.	1. Nombre de la entidad afianzadora que emitió el Seguro de Caución.
c)	Certificación original de autenticidad emitida por la entidad Afianzadora que otorgó el Seguro de Caución de Sostenimiento de Oferta.	1. Fecha de emisión.
d)	Declaración Jurada contenida en Acta Notarial.	1. Fecha de emisión.
e)	Solvencia Patronal.	1. Indicar hasta qué fecha está solvente.
f)	Fotocopia legible legalizada de los documentos siguientes:	
f.1)	Si el OFERENTE es persona individual:	
	• Testimonio de la Escritura Pública de Mandato, si fuera el caso, debidamente inscrito en los registros correspondientes.	1. Fecha de Escritura Pública de Mandato, si fuera el caso.
f.2)	Si el OFERENTE es persona jurídica:	
	• Documento Personal de Identificación -DPI-, vigente del Representante Legal o Mandatario.	1. Número de Documento Personal de Identificación -DPI-.
	• Testimonio de la Escritura Pública de Mandato, si fuera el caso, debidamente inscrito en los registros correspondientes.	1. Fecha de Escritura Pública de Mandato, si fuera el caso.
	• En caso de ser extranjeros adjuntar fotocopia legible legalizada de pasaporte completo vigente.	1. Número de Pasaporte.
f.3)	Autorización otorgada al distribuidor por el titular o Representante Legal de la casa matriz donde tenga la representación comercial para ofrecer y comercializar el OBJETO.	1. Fecha de emisión.

DOCUMENTO		**PARÁMETROS QUE DEBERÁ INGRESAR EN EL FORMULARIO ELECTRÓNICO**
g)	Constancia Electrónica de inscripción y precalificación como proveedor del Estado que para el efecto emita el Registro General de Adquisiciones del Estado -RGAE-.	1. Número de correlativo.
h)	Constancia de Inscripción al Registro Tributario Unificado -RTU-.	1. Número de Identificación Tributaria -NIT- del OFERENTE.
i)	Cartas de referencia que comprueben el tiempo de experiencia requerido.	1. Indique cantidad de cartas de referencia a presentar.
j)	Listado del personal nacional o extranjero que realizará la implementación, configuración y puesta en funcionamiento del EQUIPO. de acuerdo al ANEXO 6.4 de los DOCUMENTOS DE LICITACIÓN	1. Indique cantidad de documentos a presentar.
k)	Cuadro de ESPECIFICACIONES TÉCNICAS requeridas del EQUIPO, según ANEXO 6.3 de los DOCUMENTOS DE LICITACIÓN.	1. Indicar si en la OFERTA, incluye el cuadro de ESPECIFICACIONES TÉCNICAS del OBJETO -SI o NO-.
l)	Catálogos, guías de administración, manuales documentación y/o guías técnicas, que evidencien el cumplimiento de cada una de las ESPECIFICACIONES TÉCNICAS requeridas.	1. Indicar si en la OFERTA, incluye Catálogos entre otros -SI o NO-.
m)	Original de la certificación bancaria.	1. Fecha de emisión de Certificación Bancaria.
n)	Carta del OFERENTE que indique que se compromete a cumplir con lo establecido en el subnumeral 2.30 de los DOCUMENTOS DE LICITACIÓN.	1. Fecha de emisión.
o)	Original de la Constancia de la Visita realizada a la UNIDAD SOLICITANTE, de acuerdo al ANEXO 6.5.	1. Fecha de la visita.
p)	Formulario de identificación del OFERENTE.	1. Nombre del OFERENTE.
q)	Original o fotocopia legible legalizada de carta que demuestre que es proveedor con el máximo nivel de certificación autorizado por parte del fabricante del EQUIPO ofertado a nivel local como regional.	1. Fecha de emisión
r)	Fotocopia legible legalizada de los Certificados ISO requeridos.	1. Indique la cantidad de documentos a presentar.

DOCUMENTO		**PARÁMETROS QUE DEBERÁ INGRESAR EN EL FORMULARIO ELECTRÓNICO**
s)	Certificaciones del Project Manager, especialistas y técnicos establecidos en las ESPECIFICACIONES TÉCNICAS.	1. Indique la cantidad de documentos a presentar.
t)	Matriz de escalamiento según nivel de servicios establecidos en las ESPECIFICACIONES TÉCNICAS.	1. Indicar si en la OFERTA, incluye la Matriz de escalamiento según nivel de servicios -SI o NO-
u)	Fotocopia simple del cuadrante de Gartner vigente en donde aparezca la marca ofertada.	1. Indicar si en la OFERTA, incluye la fotocopia simple del cuadrante de Gartner -SI o NO-.
v)	Certificación o Constancia de Accionistas, Directivos o Socios, si el OFERENTE es persona jurídica. (**). Fotocopia legible legalizada del libro de accionistas.	1. Fecha de emisión.
w)	Solvencia o cualquier otro documento vigente que para el efecto emita la Inspección General de Trabajo del Ministerio de Trabajo y Previsión Social.	1. Fecha de emisión.
x)	Original o fotocopia legible legalizada de carta en la que certifique que posee la infraestructura necesaria local y/o regional para cubrir requerimientos de garantía de los equipos que forman parte de la solución	1. Fecha de emisión.

1. **(**)** Dicho requisito no aplica si el OFERENTE es Persona Individual, por lo que deberá colocar en el parámetro solicitado por GUATECOMPRAS el texto **NO APLICA** y no será motivo de rechazo por parte de la JUNTA.

2. En aquellos parámetros que no aplique ingresar algún dato, deberá consignarse el texto **NO APLICA** y no será motivo de rechazo por parte de la JUNTA.

6.2 FORMULARIO DE IDENTIFICACIÓN DEL OFERENTE

EVENTO DE LICITACIÓN DA No. 687-IGSS-2023

ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD, REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-

Datos del OFERENTE:

Persona Individual:
Nombre del Propietario o Mandatario:
Nombre de la Empresa:

Persona Jurídica:
Nombre del Representante Legal o Mandatario:
Razón o Denominación Social:
Nombre de la Empresa:

Dirección:
Teléfono (s) del OFERENTE:
Teléfono (s) móvil (es):
Correo electrónico:
Número de Identificación Tributaria, -NIT-:

_____

Firma del Propietario, Representante Legal o Mandatario

6.3 CUADRO DE ESPECIFICACIONES TÉCNICAS REQUERIDAS DEL EQUIPO

NOMBRE DEL OFERENTE:		
ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.1 Modulo: Descripción General de la Solución.		
Clasificación Funcional: Integración y automatización de la Solución		
Descripción de la Función	1. Se debe proveer una solución que permita integrar plataformas y herramientas de ciberseguridad en un ecosistema cooperativo que brinde interoperabilidad para proteger los diferentes vectores de ataque existentes de forma coordinada y con posibilidad de escalar de forma modular de acuerdo con lo expresado por la organización Gartner bajo el concepto de "Arquitectura de malla o tejido de seguridad cibernética" o "Cybersecurity Mesh Architecture" en inglés.	
	2. La Solución ofertada debe tener capacidades de integración y automatización dentro de las plataformas, herramientas de red y ciberseguridad que la conforman.	
	3. La Solución ofertada debe considerar como mínimo la protección de dispositivos (endpoints y servidores), aplicaciones, la red, el centro de datos como mínimo.	
	4. La Solución debe contar con herramientas contra amenazas persistentes de acuerdo con lo descrito en las especificaciones técnicas de los elementos necesarios solicitados.	
	5. La Solución debe contar con herramientas unificadas de monitoreo capaces de generar reportería y tableros que permitan la visibilidad de las amenazas que sean descubiertos por las herramientas de seguridad que la componen. Las herramientas de monitoreo deberán dar visibilidad del estado de salud de los componentes de la Solución, así como considerar la integración de indicadores de compromiso que puedan ser utilizados por otros elementos de la Solución para identificar amenazas.	

	6. La Solución debe contar con un subsistema de identificación y accesos para las personas responsables de gestionar y monitorear los componentes de esta.	[ ]
	7. No se considerarán las ofertas que propongan una arquitectura con silos o islas de protección que no son capaces de interactuar y automatizar tareas de defensa en conjunto con las otras herramientas propuestas como parte de la arquitectura.	[ ]
	8. El OFERENTE deberá considerar los servicios profesionales necesarios para realizar las integraciones y automatizaciones que a continuación se describen como mínimo, esto como beneficio de la arquitectura integral requerida.	[ ]
Se requiere de las siguientes Integraciones		
1. El equipo de seguridad de red (Firewall) debe integrarse a la plataforma de Sandboxing, como mínimo los firewalls incluidos en la Solución deben ser capaces de enviar archivos sospechosos a la plataforma de Sandboxing y la misma debe ser capaz de analizarlos y realizar pruebas en ambiente aislado a la red y con esto determinar si son maliciosos o no. En caso se confirme que son maliciosos debe retroalimentar a los demás elementos de la Solución para que puedan identificar la amenaza de día cero y bloquear las siguientes descargas del archivo malicioso.		[ ]
2. El equipo de balanceo de carga de aplicaciones y el Firewall de Aplicaciones Web (WAF) debe integrarse a la solución de Sandboxing, para evitar el envío de amenazas de día 0 en la carga de archivos a los servidores que estará protegiendo.		[ ]
3. Detección y respuesta extendida para amenazas avanzadas en el Endpoint o EDR debe integrarse a la solución de Sandboxing de forma nativa, para evaluar archivos sospechosos e identificar amenazas de día cero en conjunto, al detectar la amenaza debe retroalimentar a los demás componentes de la Solución incluyendo al EDR para que puedan aislar la amenaza y mitigar o de ser posible eliminar el riesgo de forma proactiva.		[ ]
4. El Control de Acceso a la Red (NAC) debe ser capaz de recibir alertas de seguridad del Firewall, con la finalidad de automatizar la respuesta y aislar a la computadora a nivel de capa 2, colocándolo en una VLAN de cuarentena.		[ ]
5. El SIEM debe poder enviar al Firewall direcciones IP maliciosas identificadas en la red, con la finalidad de automatizar el bloqueo a nivel de Firewall de la amenaza .		[ ]

6. Los equipos de seguridad de red (Firewall) debe poder integrarse con la plataforma de NDR por protocolo ICAP para enviar archivos, logrando así que NDR pueda identificar la amenaza y automatizar la respuesta con el Firewall, bloqueando así el malware de manera más efectiva.	
7. El Control de Acceso a la Red "NAC", protección de endpoint, doble factor de autenticación y Firewalls deben poder integrarse tanto con la plataforma de analítica que ya tiene el instituto como con el SIEM que se está solicitando en este evento.	

MODELO DEL EQUIPO:			
MARCA DEL EQUIPO:			
FABRICANTE:			
ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)**	**No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS**
4.2 Módulo: Dos (2) Dispositivos Next Generation Firewall para seguridad lógica de redes internas y Data Center			
Clasificación Funcional: Firewall de protección de redes internas y Data Center.			
Descripción de la Función	1. Puerto de administración dedicada, fuera de banda o similar de tipo RJ45		
	2. Puerto de consola serial		
	3. 2 puertos 10 GE / GE RJ45		
	4. 2 puertos 25GE SFP28/ 10GE SFP+		
	5. 30 puertos 25GE SFP28/ 10GE SFP+/ GE SFP		
	6. 6 puertos 100GE QSFP28/ 40GE QSFP+ Slots		
	7. Rendimiento de IPS 72 Gbps		
	8. Rendimiento de NGFW 65 Gbps		
	9. Rendimiento de protección de amenazas 63 Gbps		
	10. Rendimiento de inspección SSL 63 Gbps		
	11. Latencia de Firewall 4 microsegundos		
	12. Rendimiento de Firewall de 630 Mpps		

	13. Sesiones concurrentes TCP 140 millones como mínimo		
	14. Nuevas sesiones/segundo 1 millón		
	15. Políticas de Firewall 200,000 como mínimo		
	16. Rendimiento de control de aplicaciones 135 Gbps		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
	17. El equipo debe ser líder en el cuadrante mágico de Gartner para WAN Edge y Network Firewalls.	

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)	No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS
	18. Soporte para la creación de dominios virtuales		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
	19. El equipo debe ser compatible con plataforma de logs y gestión de Firewalls actualmente en el Instituto.	

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)	No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS
	20. Soporte de alta disponibilidad en modos Activo-Activo, Activo-Pasivo y Clustering		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
	21. 2 unidades de rack con kit de montaje y tornillos incluidos para su instalación	

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)	No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS
	22. Fuentes de poder intercambiables en caliente (hot-swap) y redundantes 100-240V AC, 50-60Hz	[ ]	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
A. Funcionalidades Generales	[ ]
B. Control de política por Firewall	[ ]
C. Control de Aplicación	[ ]
D. Prevención de Amenazas	[ ]
E. Identificación de Usuarios	[ ]
F. Manejo de Tráfico (Traffic Shapping)	[ ]
G. VPN	[ ]
H. ACCESORIOS INCLUIDOS	[ ]

MODELO DEL EQUIPO: [ ]			
MARCA DEL EQUIPO: [ ]			
FABRICANTE: [ ]			
ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)**	**No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS**
4.3 Módulo: Dos (2) Dispositivos Next Generation Firewall para protección de Perímetro			
Clasificación Funcional: Firewall Perimetral			
Descripción de la Función	1. Puerto de administración dedicada, fuera de banda o similar de tipo RJ45	[ ]	[ ]

	2. Puerto de consola serial	[ ]	[ ]
	3. 16 puertos GE RJ45	[ ]	[ ]
	4. 8 puertos GE SFP	[ ]	[ ]
	5. 12 puertos 25GE SFP28 o 10 GE SFP+	[ ]	[ ]
	6. 4 puertos 40 GE QSFP+	[ ]	[ ]
	7. Rendimiento de IPS 17 Gbps	[ ]	[ ]
	8. Rendimiento de NGFW 11 Gbps	[ ]	[ ]
	9. Rendimiento de protección de amenazas 9 Gbps	[ ]	[ ]
	10. Rendimiento de inspección SSL 12 Gbps	[ ]	[ ]
	11. Latencia de Firewall 4 microsegundos	[ ]	[ ]
	12. Rendimiento de Firewall de 200 Mpps	[ ]	[ ]
	13. Sesiones concurrentes TCP 8 millones como mínimo	[ ]	[ ]
	14. Nuevas sesiones/segundo 500,000	[ ]	[ ]
	15. Políticas de Firewall 10,000 como mínimo	[ ]	[ ]
	16. Rendimiento de control de aplicaciones 24 Gbps	[ ]	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
	17. El equipo debe ser líder en el cuadrante mágico de Gartner para WAN Edge y Network Firewalls.	[ ]
	18. El equipo debe ser compatible con la plataforma de logs y gestión de Firewalls actualmente en el Instituto.	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)	No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS
	19. Soporte para la creación de dominios virtuales	[ ]	[ ]
	20. Soporte de alta disponibilidad en modos Activo-Activo, Activo-Pasivo y Clustering	[ ]	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
	21. 2 unidades de rack con kit de montaje y tornillos incluidos para su instalación	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)	No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS
	22. Fuentes de poder intercambiables en caliente (hot-swap) y redundantes 100-240V AC, 50-60Hz	[ ]	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
A. Funcionalidades Generales	[ ]
B. Control de política por Firewall	[ ]
C. Control de Aplicación	[ ]
D. Prevención de Amenazas	[ ]
E. Filtrado URL	[ ]
F. Identificación de Usuarios	[ ]
G. Manejo de Tráfico (Traffic Shapping)	[ ]
H. VPN	[ ]
I. Accesorios Incluidos	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.4 El EQUIPO debe incluir las siguientes funcionalidades y software, como se describe a continuación:	
Funcionalidades para integrar	
Debe integrar una solución de Protección de correo electrónico, Antispam.	[ ]
Debe ser una solución basada en la nube para 13,000 cuentas	[ ]
Debe contar con esquema de HA brindado por el fabricante de la solución	[ ]
Debe tener escalabilidad, es decir permitir el escalamiento de buzones de correo.	[ ]

La institución no se debe preocupar por temas de infraestructura siendo una solución SaaS	[ ]
La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.	[ ]
La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent).	[ ]
La solución debe ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidas.	[ ]
Debe poder ser instalado en forma de proxy SMTP transparente, para el análisis de correo saliente, buscando evitar el reporte en Blacklist	[ ]
Debe tener disponible un API basado en REST para fines de monitoreo, automatización y orquestación.	[ ]
El licenciamiento debe ser basado por cantidad de buzones a proteger.	[ ]
A. Funcionalidades Generales	[ ]
B. Funcionalidades de Antispam	[ ]
C. Funcionalidades de Sesion	[ ]
D. Funcionalidades de gestion	[ ]
E. Funcionalidades de DLP	[ ]
F. Funcionalidades de Cifras	[ ]
G. Funcionalidades de Regulación	[ ]
H. Funcionalidades de Log y Reportería	[ ]
I. RFCs Soportadas	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.4.1	
Funcionalidades para integrar	
Protección avanzada contra amenazas persistentes "Sandbox"	[ ]
La cual tendrá como función principal la detonación Remota de amenazas de día Cero.	[ ]
A. Deberá contener las siguientes características	
1. Soporte para 22 máquinas virtuales para pruebas de sandbox como mínimo, entre ellas Windows 8, Windows 10 y 5 licencias de Office.	[ ]
2. Soporte para inteligencia de amenazas como Antivirus, IPS, Web Filtering, File query y seguridad industrial.	[ ]

3. 4 interfaces de 1Gbps RJ-45	
4. 2 interfaces de 10Gbps SFP+	
5. 2 discos de 1 TB	
6. Fuentes de poder intercambiables en caliente (hot-swap) y redundantes	
B. Funciones de protección generales	
C. Funciones de Protección contra Amenazas Persistentes	
D. Funciones de Visibilidad	

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.4.2		
Control de Accesos a la Red "NAC"		
Debe tener la funcionalidad del permitir el control de acceso a la red y perfilamiento de dispositivos		
1.	La solución debe contar con las licencias en su implementación para al menos, 15,000 dispositivos conectados simultáneamente, estas deben ser perpetuas.	
2.	Debe ser del tipo VM, compatible con el hipervisor del Instituto, permitiendo el uso de 20 vCPU y 32 GB de memoria RAM.	
3.	La solución debe ser escalable, permitiendo instalaciones de múltiples dispositivos físicos adicionales coordinados para crecimiento.	
4.	La solución debe permitir el crecimiento mediante la compra de licencias por cantidad de dispositivos y estas deben ser perpetuas y permitir distintos niveles de operación (visibilidad, control, cumplimiento).	
A. Visibilidad a nivel de Red		
B. Visibilidad a Nivel de Endpoint		
C. Visibilidad a nivel de usuario		
D. Funciones de automatización y control requeridas		
E. Respuesta a Incidentes		
F. Integración requerida con otras soluciones		
G. Gestión de NAC		
H. Reportería que debe incluir la solución		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.4.3	

Protección basada en señuelos para bloqueo de amenazas internas y externas "HoneyPot"		[ ]
1.	Los derechos de uso de licencia (protección contra amenazas basada en engaños) deberán tener una capacidad de 5 (cinco) VLANs (redes virtuales) y hasta 128 (ciento veintiocho) redes.	[ ]
2.	Los derechos de uso de licencias (protección contra amenazas basada en engaños) deberán tener la capacidad de emular hasta 2(dos) instancias de máquinas virtuales del Sistema Operativo Windows 10 y 2 (dos) instancias de máquinas virtuales del sistema operativo Linux.	[ ]
3	Los derechos de uso de licencias (protección contra amenazas basada en engaños) deberán estar diseñados para engañar, exponer y eliminar ataques avanzados evitando que el programa maligno se propague, brindando visibilidad a la actividad maliciosa que puede haber pasado los controles de seguridad tradicionales automatizando la creación de máquinas virtuales engañosas llamadas señuelos para proporcionar una capa interna de protección para atraer y exponer a los atacantes que han penetrado en la red.	[ ]
4.	El software de protección contra amenazas basada en engaños deberá engañar a las amenazas externas e internas con instancias de máquinas virtuales engañosas también conocidas como señuelos, administradas desde una ubicación centralizada siendo capaz de emular sistemas Windows, Linux, VPN, Medical IoT y SCADA con servicios que no se puedan distinguir de los activos reales, como: servidores de producción y señuelos integrados en dispositivos diseñados para descubrir a los atacantes.	[ ]
5.	El software de protección contra amenazas basada en señuelos deberá exponer la actividad de los piratas informáticos con detección temprana y precisa, alertas procesables habilitadas a través del seguimiento y la correlación de las tácticas, herramientas y procedimientos de un atacante y la notificación activa a través de la interfaz de usuario web, correo electrónico, registros de logs y eventos a través de la infraestructura del instituto.	[ ]
6.	El software de protección contra amenazas basada en señuelos deberá eliminar las amenazas detectadas mediante la automatización de la respuesta ante amenazas contra Firewalls, NAC y soluciones de seguridad de terceros a través la implementación del concepto de security mesh presentado por Gartner donde exista integración nativa y capacidades de automatización con otros elementos de la solución de ciberseguridad.	[ ]
7.	El software de protección contra amenazas basadas en señuelos deberá soportar los siguientes servicios: SSL VPN, SSH, SAMBA, SMB, RDP, HTTP/S, SQL, GIT, DICOM, Telnet, FTP, TFTP, SNMP, MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, EtherNet/IP, DNP3, JET-DIRECT, RTSP, UPnP, CDP y TCP.	[ ]

8.	El software de protección contra amenazas basado en señuelos deberá instalarse en una plataforma de hipervisor compatible con la infraestructura del instituto.	

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.4.4	
Gestión y Monitoreo de la Solución de Ciberseguridad	
A. Arquitectura de la plataforma de gestión de la Solución de ciberseguridad.	
B. Arquitectura de la plataforma de monitoreo, análisis y reportería de la Solución de ciberseguridad.	

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.4.5		
Gestión de Eventos e Incidentes de Seguridad – SIEM		
Debe tener la funcionalidad de Monitoreo y correlación de incidentes de seguridad.		
1.	Debe ser del tipo VM, compatible con el Hipervisor del Instituto.	
2.	Soporte para recepción de 18,000 EPS	
3	Soporte para 1600 dispositivos	
4.	Soporte monitoreo y FIM para 200 servidores Windows	
5.	Soporte monitoreo y FIM para 50 servidores Linux	
6.	Soporte de IOC para 1600 dispositivos	
A. Requerimientos no funcionales		
B. Requerimientos generales de la solución		
C. Funciones de descubrimiento y monitoreo		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.4.6		
Acceso a la Red basado en "Cero Confianza" con protección de endpoint.		
Se requiere de contar con una plataforma dentro de la solución para acceso remoto a la red basado en Cero Confianza "Zero Trust Network Access", Protección Avanzada de Endpoint, Filtrado de Contenido y Gestión de Vulnerabilidades.		
1.	Se debe incluir licenciamientos para 11,500 endpoints	
2.	Debe permitir la gestión centralizada de todos los endpoints	

A. Funciones Generales	
B. Funcionalidades de Filtrado de Contenido Web	
C. Funcionalidades de Firewall de Aplicación	
D. Funcionalidades de VPN SSL	
E. Funcionalidades de VPN IPSec	
F. Funcionalidades de Scanner de Vulnerabilidades	
G. Funcionalidades de Gestión	

MODELO DEL EQUIPO:			
MARCA DEL EQUIPO:			
FABRICANTE:			
ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)**	**No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS**
4.5 Módulo: Dos (2) Balanceadores de aplicaciones y web application firewalls			
Clasificación Funcional: Balanceo de aplicaciones y Firewall para aplicaciones Web			
Descripción de la Función	1. Los equipos deberán soportar los siguientes modos de despliegue: - Transparente. - Proxy Inverso. - One-Arm. - Router. - Direct Server Return. - Aceleración SSL por Software		
	2. La solución deberá soportar al menos los siguientes interfaces: - 8 interfaces 1GE SFP. - 12 interfaces 10GE QSFP+.		
	3. Throughput L4 de 60 Gbps		
	4. Throughput L7 de 35 Gbps.		
	5. 1,200,000 Conexiones por Segundo L4.		
	6. 4,000,000 Peticiones HTTP por segundo L4.		
	7. 72,000,000 Conexiones Concurrentes L4.		
	8. 280,000 conexiones por Segundo L7 (1:1).		

	9. 40,000 conexiones por Segundo SSL (claves 2k, cifrado AES256-SHA).	[ ]	[ ]
	10. 25 Gbps Throughput Compresión.	[ ]	[ ]
	11. 240 GB SSD de almacenamiento.	[ ]	[ ]
	12. Soporte de 10 instancias virtuales.	[ ]	[ ]
	13. 64 GB de Memoria.	[ ]	[ ]
	14. Soporte de integración con HSM de SafeNet.	[ ]	[ ]
	15. Soporte de instancias virtuales dentro del mismo equipo, pudiendo tener configuraciones y límites de rendimientos por cada una de dichas instancias.	[ ]	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
A. Gestión	[ ]
B. Alta Disponibilidad	[ ]
C. Routing Dinámico y Servicios	[ ]
D. Calidad de Servicio (QoS)	[ ]
E. Instancias Virtuales	[ ]
F. Licenciamiento	[ ]
G. Balanceo de Carga Local (SLB) y Optimización de Aplicaciones	[ ]
H. Balanceo de Aplicaciones, Persistencia, Reescritura/Enrutado en base a Contenidos y NAT	[ ]
I. Optimización de aplicaciones	[ ]
J. Soporte SSL/TLS	[ ]
K. Objetos Dinámicos	[ ]
L. Balanceo de Carga Global (GSLB)	[ ]
M. Balanceo de Carga de Líneas (LLB)	[ ]
N. Autenticación de Usuarios	[ ]
O. Funcionalidades de Seguridad	[ ]
P. Firewall de Aplicaciones Web (WAF)	[ ]
Q. Monitoreo e Informes	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.5.1	

Autenticación de doble factor.		[ ]
1.	Licenciado para soportar al menos 2000 usuarios locales o remotos	[ ]
2.	Licenciado con 2000 tokens	[ ]
3.	Licenciado para permitir al menos 150 grupos de usuarios	[ ]
4.	Debe ser de tipo vm y debe estar soportado en el hipervisor del instituto.	[ ]
A. Funciones Generales		[ ]
B. Funcionalidades de autenticación		[ ]
C. Funcionalidades de Control por Puerta		[ ]
D. Funcionalidades de Autoridad Certificadora		[ ]
E. Funcionalidades de Single Sign-On		[ ]
ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.5.2		
Detección y respuesta extendida para amenazas avanzadas en el Endpoint.		[ ]
La solución para la detección y respuesta extendida de amenazas en computadoras y servidores clave, sin necesidad de firmas, deberá incluir el licenciamiento necesario para proteger al menos 1000 dispositivos, con la solución de detección y respuesta.		[ ]
A. Funcionalidades Generales		[ ]
B. Funcionalidades de detección de malware		[ ]
C. Funcionalidades de prevención de malware		[ ]
D. Funcionalidad post-infección requerida		[ ]
E. Respuesta de incidentes		[ ]
F. Descubrimiento de vulnerabilidades y comunicaciones		[ ]
G. Cumplimiento, Integración y Consola de Gestión.		[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.5.3		
Orquestación de seguridad, automatización y respuesta a incidentes		[ ]
1.	Se requiere la automatización de respuesta y resolución de incidentes de seguridad detectados por SIEM u otras soluciones que forman parte de la plataforma.	[ ]

2.	Debe ser predecible de costear, con una métrica basada sólo en el número de usuarios, los usuarios pueden ser usuarios nombrados o concurrentes, de modo que con 1 usuario concurrente puede permitir la conexión de hasta 10 personas o más, pero no al mismo tiempo.	
3.	La solución debe admitir la concesión de licencias cuando se despliegue en redes air-gapped.	
4.	El licenciamiento debe ser para 4 usuarios concurrentes.	
A. Arquitectura		
B. Funcionalidades Generales		
C. Reportería		
D. Analítica y Alertas		
E. Playbooks		
F. Conectores para integración con terceros		
G. Indicadores de compromiso		
H. Pistas de Auditoría		
I. Gestión de usuarios y RBAC		
J. Capacidades de Despliegue		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.5.4		
Detección y respuesta extendida para amenazas avanzadas en la red		
Se requiere la de detección de amenazas en la red con base en inteligencia artificial y aprendizaje de máquina.		
1.	Soportar un máximo de 32 vCPU.	
2.	Soportar un máximo de memoria RAM de 256 GB	
3.	Soporta 2 factores para el inicio de sesión administrativa	

4.	Contar con capacidad de almacenamiento de 4 TB	
5.	Admite administradores remotos LDAP/RADIUS	
6.	Admite RBAC para el acceso administrativo	
7.	La solución debe ser compatible con el hipervisor VMware y KVM	
A. Capacidades de detección de amenazas		
B. Capacidades de gestión del despliegue		
C. Requisitos de registro e información		
D. Integraciones de seguridad		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.5.5		
Gestión de la Seguridad para el Acceso a la Nube, para protección de ambientes de Microsoft 365.		
Se requiere la protección de ambientes de ofimática basada en nube como la aplicación Microsoft 365 y otros ambientes de nube de software como servicio		
1.	Capacidad de analizar al menos 500 cuentas de Office 365	
2.	La solución debe ser de tipo SaaS	
3.	Visibilidad centralizada	
4.	Extiende la protección de la seguridad de la nube a las instalaciones de la empresa	
5.	Simplificar el cumplimiento de muchas normas del sector, como como PCI DSS, HIPAA, SOC2 y GDPR con políticas e informes predefinidos e informes predefinidos	
6.	Supervisar los comportamientos y actividades de los usuarios y gestionar los derechos de los usuarios	
7.	Prevención de pérdida de datos (DLP) y herramientas de detección de amenazas	
8.	Integración con Office365, Google, Yammer, Teams, Microsoft Azure, Dropbox, Google Drive, Service Now, Github.	
9.	Debe integrarse con la solución actual de recolección de logs de Firewall para identificar Shadows IT dentro de la red.	

10.	Integración con las siguientes aplicaciones de Microsoft: -Microsoft Teams -Microsoft OneDrive -Microsoft sharepoint - Azure Active Directory	
A. Visibilidad		
B. Seguridad de datos y protección contra amenazas		
C. Cumplimiento		

MODELO DEL EQUIPO:			
MARCA DEL EQUIPO:			
FABRICANTE:			
ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)**	**No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS**
4.6 Módulo: Cuatro (4) conmutadores para interconexión de la Solución de Ciberseguridad			
Clasificación Funcional: Conmutación de paquetes en la Solución de Ciberseguridad			
Descripción de la Función	1. Equipo de grado Enterprise		
	2. Capacidad para L2 y L3		
	3. MDI/MDIX Auto-crossover		
	4. Soporte de spanning tree IEEE 802.1d, IEEE 802.1w, IEEE 802.1s		

	5. Soporte para medios y velocidades de transmisión según estándares IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3ab 1000Base-T y IEEE 802.3ae 10 Gigabit Ethernet, según aplique para los puertos requeridos en las características específicas del equipo.		
	6. Puertos con auto negociación de velocidad y dúplex		
	7. Soporte para Link Aggregation IEEE 802.3ad y IEEE 802.1AX		
	8. Soporte de medios y velocidades de transmisión definidas en los estándares:		
	9. Soporte para VLAN Tag IEEE 802.1Q		
	10. Soporte para manejo de Jumbo Frames		
	11. Soporte para SNMP versiones 1, 2 y 3.		
	12. Soporte para sFlow		
	13. Soporte para autenticación basada en estándar 802.1x (Basada en puerto y MAC), con asignación dinámica de VLAN,		
	14. Administración mediante acceso por SSH, HTTPS y consola serial (En el caso de conexión a consola serial, se debe proveer cable especifico de la marca y, de ser necesario, los convertidores necesarios para conexión a equipos con puertos USB-A y USB-C, con soporte para los sistemas operativos actuales)		
	15. Soporte de configuración y monitoreo mediante REST API’s		

	16. Soporte para DHCP-Snooping		
	17. Soporte para configuración de al menos 64 rutas estáticas		
	18. Soporte para implementación de ACL's		
	19. Soporte para hacer Port Mirroring		
	20. Soporte para QoS basado en estándar IEEE 802.1p y basado en Type of Service		
	21. Soporte para SNTP		
	22. Soporte para DHCP Relay		
	23. Soporte para Dynamic ARP Inspection		
	24. Soporte de funcionalidades de LLDP IEEE 802.1ab		
	25. Soporte para MCLAG (o característica similar que permita soportar arreglos de alta disponibilidad)		
	26. Soporte para descarga y carga de archivos al equipo mediante TFTP, FTP, y GUI		
	27. Administración centralizada de VLANs desde un dispositivo de gestión		
	28. Capacidad de aplicar políticas entre VLANs a nivel de aplicación, IP o puertos TCP/UDP desde un dispositivo de gestión		

	29. Capacidad de integrarse para la gestión con dispositivos de seguridad perimetral como cortafuegos		
	30. Debe soportar los siguientes modos de administración: - Stand-alone - Por software o appliance de gestion - Cloud management		

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
A. Características específicas del equipo	

MODELO DEL EQUIPO:			
MARCA DEL EQUIPO:			
FABRICANTE:			
ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**ESPECIFICACIONES TÉCNICAS OFERTADAS (DESCRIPCIÓN QUE CORRESPONDE SEGÚN EL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS)**	**No. DE PÁGINA DEL CATÁLOGO, GUÍA DE ADMINISTRACIÓN, MANUAL DOCUMENTACIÓN Y/O GUÍAS TÉCNICAS**
4.7 Módulo: Dos (2) conmutadores para recepción de WAN e Internet			
Clasificación Funcional: Conmutadores para recepción de enlaces de WAN y de Internet e integración con Firewall de Perímetro			
Descripción de la Función	1. Equipo de grado Enterprise		
	2. Capacidad para L2 y L3		
	3. MDI/MDIX Auto-crossover		

	4. Soporte de spanning tree IEEE 802.1d, IEEE 802.1w, IEEE 802.1s		
	5. Soporte para medios y velocidades de transmisión según estándares IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z 1000Base-SX/LX, IEEE 802.3ab 1000Base-T y IEEE 802.3ae 10 Gigabit Ethernet, según aplique para los puertos requeridos en las características específicas del equipo.		
	6. Puertos con auto negociación de velocidad y dúplex		
	7. Soporte para Link Aggregation IEEE 802.3ad y IEEE 802.1AX		
	8. Soporte de medios y velocidades de transmisión definidas en los estándares:		
	9. Soporte para VLAN Tag IEEE 802.1Q		
	10. Soporte para manejo de Jumbo Frames		
	11. Soporte para SNMP versiones 1, 2 y 3.		
	12. Soporte para sFlow		
	13. Soporte para autenticación basada en estándar 802.1x (Basada en puerto y MAC), con asignación dinámica de VLAN		

	14. Administración mediante acceso por SSH, HTTPS y consola serial (En el caso de conexión a consola serial, se debe proveer cable especifico de la marca y, de ser necesario, los convertidores necesarios para conexión a equipos con puertos USB-A y USB-C, con soporte para los sistemas operativos actuales)		
	15. Soporte de configuración y monitoreo mediante REST API's		
	16. Soporte para DHCP-Snooping		
	17. Soporte para configuración de al menos 64 rutas estáticas		
	18. Soporte para implementación de ACL's		
	19. Soporte para hacer Port Mirroring		
	20. Soporte para QoS basado en estándar IEEE 802.1p y basado en Type of Service		
	21. Soporte para SNTP		
	22. Soporte para DHCP Relay		
	23. Soporte para Dynamic ARP Inspection		
	24. Soporte de funcionalidades de LLDP IEEE 802.1ab		
	25. Soporte para MCLAG (o característica similar que permita soportar arreglos de alta disponibilidad)		
	26. Soporte para descarga y carga de archivos al equipo mediante TFTP, FTP, y GUI		
	27. Administración centralizada de VLANs desde un dispositivo de gestión		

	28. Capacidad de aplicar políticas entre VLANs a nivel de aplicación, IP o puertos TCP/UDP desde un dispositivo de gestión	[ ]	[ ]
	29. Capacidad de integrarse para la gestión con dispositivos de seguridad perimetral como cortafuegos	[ ]	[ ]
	30. Debe soportar los siguientes modos de administración: - Stand-alone - Por software o appliance de gestión - Cloud management	[ ]	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
A. Características específicas del equipo	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.8 Módulo: Servicios de soporte técnico y garantía de hardware y software.		
Clasificación Funcional: Soporte técnico y garantía de hardware y software		
Descripción de la Función	1. La Solución de ciberseguridad y todos sus componentes deberán incluir soporte y garantía de fábrica 7x24x365 por un plazo de tres (3) años contados a partir de la fecha de emisión del acta de recepción.	[ ]
	2. El soporte y la garantía deberán de cubrir tanto a los equipos físicos como dispositivos virtuales y el licenciamiento de software necesario para el funcionamiento descrito para cada plataforma sin importar si se trata de un licenciamiento perpetuo o por suscripción.	[ ]

	3. Si los equipos propuestos requieren acceso a los motores de inteligencia contra amenazas del fabricante, el servicio de soporte y garantía se debe incluir el licenciamiento o la suscripción necesaria para dichos servicios de tal manera que se posea el acceso a estas bases de conocimientos por al menos tres (3) años contados a partir de la fecha de emisión del acta de recepción.	[ ]
	4. El centro de atención de llamadas de soporte o garantía deberá operar bajo el formato de tiempo 7x24x365.	[ ]
	5. La atención a los incidentes por parte del fabricante deberá ser por medio de correo electrónico, llamada telefónica o chat.	[ ]
	6. El servicio de soporte y garantía debe incluir el reemplazo de partes en caso de una falla.	[ ]
	7. El servicio debe incluir acceso irrestricto a la documentación del fabricante, así como a la base de conocimientos de problemas conocidos.	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
A. Características avanzadas del servicio	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
Servicio de soporte técnico	

Servicio de soporte de incidentes y nuevas configuraciones	1. El OFERENTE deberá incluir el servicio de soporte con una disponibilidad de 24x7x365, para todos los componente incluidos en el presente documento, incluyendo soporte a incidentes, configuraciones nuevas y reconfiguraciones de los componentes después de implementados, designando un ingeniero VIP, el cual deberá llevar el historial y administración de dicho soporte, manejando en conjunto con el equipo de tecnología del INSTITUTO la gestión de cambios	

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO		**INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE**
4.9 Módulo: Servicio de implementación de la Solución de ciberseguridad		
Clasificación Funcional: Servicio de instalación, configuración e integración de la Solución de ciberseguridad		
Descripción de la Función	1. El oferente debe considerar que la Solución de ciberseguridad deberá quedar completamente funcional, protegiendo la infraestructura del Instituto. Esto implica que al menos deben considerarse las siguientes etapas: - Planeación - Diseño - Implementación - Pruebas (HA, Failover, Conectividad, funcionamiento de las herramientas de seguridad). - Documentación	
	2. El proyecto debe estar gestionado al menos por una persona con el rol de Project Manager por parte del oferente para manejo efectivo de la comunicación y coordinación con el equipo de trabajo del lado del Instituto. El Project Manager debe estar certificado por PMI o por SCRUM y deberá contar con al menos 2 años de experiencia en la gestión de proyectos de tecnología.	

	3. Para el despliegue de la Solución se deben incluir al menos cinco (5) especialistas, parte del equipo local y/o regional del OFERENTE, certificados por el fabricante como expertos en seguridad de redes nivel "Profesional" enfocado en servicios de ingeniería postventa, no se aceptan certificaciones de ventas o preventas.	[ ]
	4. Para el despliegue de la Solución se debe incluir al menos tres (3) especialistas, parte del equipo local y/o regional del OFERENTE, certificados por el fabricante como expertos en seguridad de redes nivel "Arquitectura" enfocado en servicios de postventa, no se aceptan certificaciones de ventas o preventas.	[ ]
	5. El servicio de implementación debe incluir al menos las siguientes etapas	[ ]
	Planeación:	
	6. Reunión inicial del proyecto (Kick-off) para la presentación del equipo de trabajo asignado y definición de cronograma.	[ ]
	7. Dimensionamientos previos a los sitios de instalación para definición de asignación de recursos físicos y materiales necesarios para la instalación de los equipos.	[ ]
	8. Elaboración de la planeación para la instalación y configuración de toda la solución de este RFP	[ ]
	9. Reuniones presenciales de seguimiento del proyecto, en las que se definirá el avance del proyecto y se informara si existirán cambios al cronograma indicando el responsable asociado	[ ]

	Diseño:	
	10. Levantamiento de información de las configuraciones actuales de los equipos y de la topología de la red para:	[ ]
	11. Elaboración del diseño de segmentación lógica de la solución de CyberSecurity	[ ]
	12. Elaboración de documentos de ingeniería	[ ]
	Actividades de Implementación:	
	13. Instalación física de todos los equipos contemplados en este proceso de licitación en los espacios indicados por el cliente	[ ]
	14. Configuración de toda la solución contemplada en este proceso con base a las políticas indicadas por el cliente	[ ]
	15.Pruebas locales de conectividad y funcionalidad de la solución.	[ ]
	16. Limpieza final de lugar.	[ ]
	17. Documentación de Cierre del proyecto	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO	INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
A. Consideraciones especiales en la prestación del servicio	[ ]

ESPECIFICACIONES TÉCNICAS REQUERIDAS POR EL INSTITUTO					INDICAR SI LO OFERTADO CUMPLE O NO CUMPLE
4.10 Requerimiento de hardware para virtualización de componentes de integración de la Solución					
La capacidad necesaria de cómputo, memoria, disco, interfaces de red y virtualización necesarias para ejecutar la Solución deberán ser incluidas bajo el concepto de llave en mano, de acuerdo con las magnitudes siguientes:					
Componente	**vCPU**	**Memoria RAM**	**Capacidad de Almacenamiento tipo NAS CON 10,000 IOPS**	**Interfaces de red dedicadas**	
Para solución de detección y respuesta extendida para amenazas avanzadas en la red	32	128 GB	4 TB	2 x 10 Gb	[ ]
Para solución de control de acceso a la red	20	32 GB	100 GB	2 x GE tipo RJ45	[ ]
Para solución de orquestación de seguridad, automatización y respuesta a incidentes	8	32 GB	1 TB	1 GE tipo RJ45	[ ]
Para Monitoreo de la Solución	16	64	16 TB	1 x GE RJ45 o 10 GE	[ ]
Para solución de autenticación de doble factor	2	8	1 TB	1 GE tipo RJ45	[ ]

Para solución de protección basada en señuelos para bloqueo de amenazas internas y externas	8	24	500 GB	1 GE tipo RJ45	[ ]
Para la gestión de la Solución	6	16	1 TB	1 GE tipo RJ45	[ ]
Para solución de Gestión de Eventos e Incidentes de Seguridad – SIEM	112	104	72 TB		[ ]

_____

Firma del Propietario, Representante Legal o Mandatario

6.4 LISTADO DEL PERSONAL PROPUESTO PARA LA IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DEL EQUIPO

DOCUMENTOS DE LICITACIÓN DA No. 687-IGSS-2023

ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD, REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-

INFORMACIÓN GENERAL	
Nombre del OFERENTE:	
Nombre Completo del Empleado:	
Profesión (Grado Académico):	

CERTIFICACIONES RECIBIDAS	
Nombre de la entidad que imparte la certificación	**Certificación obtenida**

Los documentos detallados en el apartado anterior, deben coincidir con los solicitados en la subliteral j.1) del subnumeral 2.8.

Firma del Propietario, Representante Legal o Mandatario

6.5 CONSTANCIA DE VISITA

DOCUMENTOS DE LICITACIÓN DA No. 687-IGSS-2023

ADQUISICIÓN, INSTALACIÓN, IMPLEMENTACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA (1) SOLUCIÓN INTEGRADA DE CIBERSEGURIDAD, REQUERIDA POR LA SUBGERENCIA DE TECNOLOGÍA PARA EL INSTITUTO GUATEMALTECO DE SEGURIDAD SOCIAL -IGSS-

Para efectos del Evento de Licitación DA No. 687-IGSS-2023, se extiende la presente el día ___ de____ de _____ de 20____, dejando constancia de lo siguiente:

El reconocimiento del área en donde se instalará el EQUIPO, con la finalidad de evaluar el ambiente operativo y considerar dentro de la OFERTA los aspectos que conllevan la correcta instalación y puesta en funcionamiento del EQUIPO.

DATOS DEL REPRESENTANTE DEL INSTITUTO:

Nombre: _____

Cargo: _____

Firma y Sello: _____

DATOS DEL OFERENTE:

Nombre del OFERENTE: _____

Nombre de la persona que hace la visita: _____

Firma: _____

7ª. Avenida 22-72, zona 1, Centro Cívico Guatemala, C. A. PBX: 2412-1224, ext. 1238

6.6 GLOSARIO

Glosario	
CEF	Formato de Evento Común (Common Event Format)
Traffic Shaping	Manejo de tráfico
Policy based routing	Ruteo basado en políticas
LOGS	Bitácoras
HA	Alta disponibilidad (high availability)
CORE O NUCLEO	Tipo de microprocesador en donde coexisten múltiples procesadores en el mismo chip.
ETHERNET	Es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones.
GB (Gigabyte)	Medida de la memoria de una computadora que es igual a 1 000 millones de bytes.
GIGABIT ETHERNET (GbE)	También conocida como GigaE, es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento.
RACK	Estante metálico cuya finalidad principal es la de alojar equipamiento electrónico, informático y de comunicaciones donde las medidas para la anchura están normalizadas para que sean compatibles con el equipamiento de cualquier marca o fabricante.
RAM	Sigla de Random Access Memory (‘memoria de acceso aleatorio’), memoria principal de la computadora, donde residen programas y datos, sobre la que se pueden efectuar operaciones de lectura y escritura.
RU	Unidades de Rack
SFP+	Son todos los tipos de transceptores utilizados para conectar un conmutador u otro dispositivo de red a un cable de cobre o fibra.
HOT-SWAP	Se utiliza para reemplazar dispositivos sin parar el funcionamiento del ordenador y/o para dispositivos internos