

Canales de radicación oficial:

Físico: Carrera 8 No 20 - 56 Piso 1 Ventanilla de Correspondencia

Digital: [gestioncorrespondencia@etb.com.co](mailto:gestioncorrespondencia@etb.com.co)



## EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S. A. E.S.P.

### BORRADOR DE TÉRMINOS DE REFERENCIA

### INVITACIÓN PÚBLICA N° 7200002519

### GRUPO: "CIBERSEGURIDAD"

BOGOTÁ D.C., DICIEMBRE DE 2025

07-07.7-F-025-v.7

01/08/2025

"Una vez impreso este documento, se considerará **documento no controlado**".

## PROCESO DE INVITACIÓN PÚBLICA ACUERDO MARCO

El presente proceso tiene como finalidad la suscripción de ACUERDOS MARCO con ALIADOS ESTRATÉGICOS para la provisión de soluciones integrales de servicios.

El propósito central es establecer una relación de colaboración con proveedores especializados que tengan la experiencia, infraestructura y capacidades técnicas necesarias. Este esquema no se limita a la prestación de un servicio específico, sino que busca permanentemente la creación de sinergias entre las partes, lo que permitirá la articulación de conocimientos, tecnologías y buenas prácticas para implementar soluciones diferenciadas que agreguen valor, optimicen costos y permitan agilidad. Asimismo, se busca que el desarrollo del contrato fomente la confianza mutua y una sólida reputación entre las partes, elementos esenciales para el desarrollo de soluciones conjuntas.

### CONSIDERACIONES

ETB tiene como misión contribuir al desarrollo social y económico del país mediante la prestación de servicios integrales tecnológicas en cumplimiento de su función empresarial y su compromiso con la transformación digital de Colombia, orienta sus esfuerzos a ofrecer soluciones que fortalezcan la conectividad, la productividad y la competitividad de los ciudadanos, las empresas y las entidades públicas a nivel distrital y nacional y privado.

ETB es un socio estratégico en la innovación de soluciones tecnológicas acorde con el dinamismo del mercado, por su experiencia y trayectoria e infraestructura y desarrollo de tecnológico, que, junto a otras instituciones, contribuye a la articulación de iniciativas que promueven la seguridad, la conectividad, la sostenibilidad y la inclusión digital en la ciudad.

ETB ha iniciado una transformación estratégica para convertirse en una empresa de tecnología digital de vanguardia, conocida como 'Techco'. Uno de los pilares fundamentales de esta estrategia es su incursión en el sector de la tecnología educativa (EdTech) para lo cual se ha dispuesto.

La unidad EdTech de ETB que es un eje estratégico fundamental para la transformación de la compañía cuyo propósito principal es contribuir al cierre de la brecha digital en Colombia mediante soluciones tecnológicas innovadoras y contenidos educativos relevantes, generando así un impacto positivo en la ciudadanía.

ETB fundamenta su gestión en principios de transparencia, Sostenibilidad y responsabilidad social, buscando generar valor para sus grupos de interés y aportar al cierre de brechas digitales a través de la expansión de infraestructura de telecomunicaciones y el acceso equitativo a la información y su propósito es ser un referente nacional en innovación tecnológica y excelencia en el servicio, impulsando el bienestar y el progreso de la comunidad.

En armonía con lo anterior, mediante el presente proceso ETB busca la conformación de un ecosistema estratégico de aliados para suscribir acuerdos marco que contribuyan al fortalecimiento de la competitividad de ETB, en consonancia con su proceso de transformación de Telco a Techco.

## ALCANCE

La conformación de un ecosistema de aliados estratégicos, a través de acuerdos marco, es un elemento clave para potenciar las integraciones que ETB realiza como experto en soluciones, apalancado en su conocimiento especializado (know-how) y experiencia técnica y operativa, que le permiten ofrecer soluciones diferenciadas y de alto valor agregado.

Uno de los pilares del Acuerdo Marco es la generación de demanda conjunta. ETB busca que el proveedor se comporte como un aliado estratégico, demostrando un compromiso proactivo con la expansión de oportunidades del mercado, aprovechando la experiencia de ETB como integrador de soluciones tecnológicas y su posicionamiento de marca.

Para materializar esta captura de mercado, el modelo priorizará socios que demuestren su compromiso a través de fondos de *marketing* (MDF). Dicho compromiso se estructurará como una co-inversión destinada a financiar estrategias de *go-to-market* (GTM), acelerar la generación de demanda y maximizar la penetración de las soluciones.

La sostenibilidad de esta transformación se fundamenta en una transferencia efectiva de conocimiento. Un socio estratégico invierte en la autonomía de su contraparte. El modelo exigirá un proceso riguroso de alta capacitación y mentoría. El objetivo es que ETB, a través de su PMO y equipos técnicos, logre la apropiación metodológica y operativa del core de las soluciones.

Las condiciones establecidas en el Acuerdo Marco de Precios podrán ser utilizadas no solo por ETB, sino también por sus filiales, subordinadas, empresas del Grupo Empresarial de ETB y aquellas en las que ETB tenga participación accionaria. Esto para los grupos en los que estas empresas no hayan sido adjudicatarias. Así mismo, podrán presentar ofertas en los grupos que apliquen.

El proyecto comprende las siguientes líneas de negocio, cuyas condiciones están diferenciadas por cada grupo:

Grupo I: Infraestructura y Software en modalidad de Servicio

Grupo II: Ciberseguridad

Grupo III: Nubes Privadas

Grupo IV: Gestión de Procesos de Negocio (BPO)

Grupo V: Desarrollo de Software según requerimientos

Grupo VI: Ciudad 360

Grupo VII: Servicios especializados

Grupo VIII: Smartphones como servicio

Grupo IX: Servicios de Conectividad Avanzada (SDWAN as a service)

Canales de radicación oficial:

Físico: Carrera 8 No 20 - 56 Piso 1 Ventanilla de Correspondencia

Digital: [gestioncorrespondencia@etb.com.co](mailto:gestioncorrespondencia@etb.com.co)



Grupo X: Smart Citys

Grupo XI: Gobierno y Empresa Inteligente

Grupo XII: E-HEALTH

Grupo XIII: EDTECH. Este grupo se compone de subgrupos independientes.

Grupo XIV: Últimas Millas de Conectividad

**El (los) Oferentes pueden presentar oferta independiente por cada grupo, según sus capacidades.**

Si bien cada grupo constituye un proceso independiente, estos se adelantarán de manera simultánea. Este esquema tiene un doble propósito: permitir a los interesados evaluar la posibilidad de integrar capacidades en los grupos a los que se postulan y, asimismo, suscribir un solo contrato con los Oferentes que resulten adjudicatarios en más de un grupo.

## CAPÍTULO I - CONDICIONES JURÍDICAS

**OBJETO:** Constituir un ecosistema estratégico de aliados, a través de acuerdos marco, con el objetivo de asegurar el suministro de soluciones integrales como servicio. Estas soluciones deberán contribuir a la transformación de ETB hacia una empresa de tecnología ("Techo"), mediante la articulación de estrategias comerciales, la participación activa en modelos de generación de demanda, la ampliación de su alcance y penetración en el mercado, y la implementación de modelos de negocio innovadores.

El alcance del presente objeto corresponde al **Grupo II "CIBERSEGURIDAD"**

**FINALIDAD DE LOS ACUERDOS MARCO:** Establecer las condiciones generales para la prestación de los servicios, con el propósito de agilizar los procesos de adquisición y atender el dinamismo de ETB en un entorno competitivo. Lo anterior se materializa mediante la definición de precios de referencia que permiten generar economías de escala en la ejecución contractual, a través de la emisión de órdenes de servicio.

**ACUERDO MARCO:** A través del proceso que derive en la consolidación de los términos de referencia definitivos, se definirán las condiciones y características técnicas para la adquisición de los servicios. Asimismo, se realizará la selección de los Aliados Estratégicos, quienes se vincularán al acuerdo marco mediante la adjudicación y celebración del contrato. El Acuerdo Marco no crea por sí mismo una obligación de compra o suministro, sino que establece las reglas para contratar de forma más ágil y eficiente.

**PRECIOS UNITARIOS:** Corresponden a los precios pactados en el contrato con base en los ítems del anexo financiero y constituyen la base para solicitar cotizaciones o adelantar negociaciones orientadas a la mejora del precio.

07-07.7-F-025-v.7

01/08/2025

"Una vez impreso este documento, se considerará **documento no controlado**".

**ORDEN DE SERVICIO:** Luego de realizado el procedimiento para la solicitud de pedido descrito en el capítulo técnico, ETB podrá considerar en asignar la orden de servicio, caso en el cual, el Aliado se obliga a la prestación del servicio en las condiciones acordadas, teniendo en cuenta que, de forma previa deberá constituir las garantías específicas que amparan cada pedido u orden de servicio.

**FORMA DE EJECUTAR EL CONTRATO:** ETB no está obligada a adquirir una cantidad mínima ni máxima de servicios, ya que ello dependerá de las órdenes de servicio que se emitan al Aliado, de conformidad con el procedimiento descrito en el capítulo técnico.

**PRECIO DEL CONTRATO:** El precio del contrato será de cuantía indeterminada, pero determinable de acuerdo con la cantidad de órdenes de servicio que se emitan y los precios unitarios pactados para las mismas.

**PRÓRROGA DEL ACUERDO MARCO:** ETB podrá prorrogar el Acuerdo Marco antes del vencimiento del plazo inicial del mismo. Para ello comunicará esta intención al Aliado para que se pronuncie al respecto. ETB podrá realizar dicho trámite, únicamente con quienes respondan positivamente a la mencionada solicitud. La prórroga se realizará mediante acuerdo suscrito entre las partes.

**HERRAMIENTA A TRAVÉS DE LA CUAL SE LLEVARÁN A CABO LAS TRANSACCIONES DERIVADAS DEL ACUERDO MARCO:** SAP ARIBA, o la herramienta que haga sus veces. Los Aliados se estarán obligados a aceptar los términos y condiciones de la herramienta.

## 1.1. CONDICIONES APLICABLES

### 1.1.1. COMUNICACIONES Y REMISIÓN DE INFORMACIÓN A TRAVÉS DE LA HERRAMIENTA SAP ARIBA.

En armonía con el propósito global de transformación digital, ETB en el marco de sus proyectos estratégicos adoptó la decisión de implementar la solución transaccional SAP ARIBA, con miras a lograr una contratación en línea con celeridad, transparencia, seguridad y oportunidad que le permitirá apalancarse en la optimización y eficiencia de sus procesos de contratación.

Bajo este entendido, el presente proceso de contratación se desarrollará a través de la herramienta SAP ARIBA. Por Consiguiente y sólo como referencia, a continuación, se detallan algunas definiciones de común utilización en la plataforma:

<b>SAP ARIBA</b>	Plataforma transaccional, que permite a ETB adelantar sus procesos de contratación, así como el relacionamiento con sus aliados y proveedores de forma colaborativa y en línea.
------------------	---

<b>Evento</b>	Campo creado en la herramienta SAP ARIBA, mediante el cual ETB recibe las ofertas de los interesados en participar en el proceso de contratación que se esté adelantando.
<b>Mensajes de Evento</b>	Bandeja de registro y envío de mensajes relacionados al proceso de contratación que se adelanta por medio de la plataforma SAP ARIBA.
<b>Oferta o Propuesta</b>	Mensaje de datos recibido por ETB para el presente proceso de selección por medio de la plataforma SAP ARIBA que contiene los ofrecimientos de un proveedor o aliado inscrito en el registro de proveedores de ETB.

Por lo anterior, todas las comunicaciones relacionadas con el presente proceso deberán presentarse dentro de los plazos descritos en el cronograma a través de la plataforma SAP ARIBA, de la siguiente manera: (i) correo electrónico de SAP ARIBA [email2workspace-prod3+etb+SR1859830310+tnel@ansmtp.ariba.com](mailto:email2workspace-prod3+etb+SR1859830310+tnel@ansmtp.ariba.com) , Constituye el canal de comunicación directo entre el proveedor y ETB, con el fin de tener soporte técnico sobre el uso de las herramientas y los siguientes canales de comunicación mediante los cuales cursarán las observaciones y se realizará la reunión informativa:

(i) enlace para las observaciones: [Enlace Preguntas](#)

(ii) enlace para la reunión informativa: [Enlace Reunión Informativa](#)

### 1.1.2. RÉGIMEN JURÍDICO DE ETB

De conformidad con lo dispuesto en el artículo 55 de la Ley 1341 de 2009 y sus modificaciones, la actuación contractual de ETB se rige por las normas de derecho privado. En consecuencia, resultan aplicables las disposiciones del Código Civil, el Código de Comercio, el Manual de Contratación, la Política Financiera y el Código de Ética, los cuales se encuentran publicados en la página web oficial de ETB: [www.etb.com.co](http://www.etb.com.co).

### 1.1.3. PUBLICACIÓN DE LOS BORRADORES DE TÉRMINOS DE REFERENCIA EN LA PÁGINA WEB DE ETB Y EN LA PLATAFORMA SAP ARIBA

- a) Los borradores términos de referencia, del cual hacen parte integral los anexos;
- b) Las observaciones y las respectivas respuestas;

### 1.1.4. CRONOGRAMA DEL PROCESO

ACTUACIÓN	FECHA
Publicación borradores de términos de referencia	23 de diciembre de 2025
Reunión informativa: 3 días	Del 7 al 9 enero de 2026, <b>Nota:</b> validar el día y la hora en el numeral 1.1.7. <b>REUNIÓN INFORMATIVA.</b>
Observaciones al borrador de los	hasta el 14 de enero de 2026

ACTUACIÓN	FECHA
términos de referencia: 2 días	
Respuesta a las observaciones: 2 días	hasta el 16 de enero de 2026
Publicación de los términos de referencia definitivos	hasta el 26 de enero de 2026

### 1.1.5. PRÓRROGAS

Los plazos establecidos en el presente capítulo para la etapa precontractual se expresan en días hábiles y podrán ser prorrogados antes de su vencimiento por el tiempo que ETB considere conveniente.

### 1.1.6. DISPOSICIONES GENERALES

Los presentes borradores de términos de referencia no tienen valor y no constituyen oferta mercantil;

- a) La información contenida en este documento sustituye totalmente aquella que pudiere haberse suministrado con anterioridad a esta invitación.

### 1.1.7. REUNIÓN INFORMATIVA.

ETB realizará una reunión informativa de manera virtual ETB realizará una reunión informativa de manera virtual, el día 7 de enero de 2026 de 10 am a 11 am, mediante la URL: [Enlace Reunión Informativa](#), con el fin de precisar el alcance del borrador de términos y condiciones.

El interesado en participar en la reunión informativa debe remitir el nombre completo y los correos electrónicos de las personas que se unirán a la reunión virtual a través de los mensajes del evento en la herramienta SAP ARIBA dentro del plazo establecido en el cronograma.

ETB analizará si las preguntas formuladas pueden o no ser respondidas en dicha reunión, acorde con la complejidad y tiempo programado para agenda. Para el caso en que las respuestas no puedan ser emitidas, en la reunión, estas serán respondidas por ETB dentro del plazo establecido para las respuestas a las observaciones formuladas por los interesados.

### 1.1.8. OBSERVACIONES A LOS BORRADORES DE LOS TÉRMINOS DE REFERENCIA

Los interesados podrán presentar observaciones a los presentes borradores de términos de referencia, atendiendo los canales establecidos en el numeral correspondiente a COMUNICACIONES Y REMISIÓN DE INFORMACIÓN A TRAVÉS DE LA HERRAMIENTA SAP ARIBA o copiando este enlace en el navegador: [Enlace Preguntas](#)

Las comunicaciones y observaciones enviadas por canales distintos a los allí mencionados no serán oponibles para ETB, hasta tanto no sean remitidas a través de los canales expresamente indicados.

## 1.2. REQUISITOS JURÍDICOS HABILITANTES (RESUMEN) QUE SERÁN EXIGIDOS EN LOS TÉRMINOS DEFINITIVOS.

- a) Anexo 1: Carta de presentación de oferta;
- b) Documentos que acrediten la existencia y representación legal;
- c) Duración de la sociedad;
- d) Autorizaciones de órgano social competente (actas de junta directiva, asamblea de socios, entre otros), cuando aplique;
- e) Poderes autenticados en Notaría Pública para oferente nacional y autenticados, apostillados, cuando se trate de documentos expedidos en el exterior; cuando aplique.
- f) Certificación en la que conste la afiliación y pago de aportes a los sistemas de salud, riesgos laborales (ARL), pensiones (AFP), cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), conforme a lo establecido en el artículo 50 de la Ley 789 de 2002, emitida por:
  - El revisor Fiscal que obre en el certificado de existencia y representación legal expedido por la Cámara de Comercio de Colombia. Dicha certificación debe estar acompañada de copia de la cédula de la tarjeta profesional, cédula de ciudadanía y el certificado vigente y actualizado de antecedentes de la Junta Central de Contadores, con fecha de expedición no mayor a tres meses con respecto a la fecha de presentación de oferta.
  - O por el representante legal o apoderado del oferente, cuando no exista la obligación de tener revisor fiscal.
- g) Certificación emitida por la ARL donde conste el nivel de cumplimiento con un porcentaje mínimo del 85% del sistema, dicha certificación debe estar vigente en la fecha de su presentación, considerando la última modificación o actualización efectuada en la ARL. Según aplique para proveedor nacional o con sucursal establecida en Colombia.
- h) Certificado REDAM del representante que suscriba la carta de presentación de oferta, conforme a lo exigido en la Ley 2097 de 2021 y en su Decreto Reglamentario 1310 de 2022. El certificado debe contar con una fecha no mayor a tres (3) meses.

Lo anterior, con observancia de cada uno de los requisitos exigidos en el presente capítulo.

### 1.2.1. CAPACIDAD, Y REPRESENTACIÓN LEGAL

El interesado en participar debe tener en cuenta que, en los términos de referencia definitivos, serán exigidos los siguientes requisitos relacionados con la capacidad jurídica.

- i. Que el objeto social le permite presentar oferta en concordancia con el objeto del GRUPO relacionado en el objeto del presente documento.
- j. La duración de la sociedad debe abarcar la vigencia total del contrato y un año más; a partir de la fecha en que la oferta sea presentada.
- k. El representante legal o apoderado deberá estar debidamente facultado y para comprometerla en la presentación de la oferta, la celebración, ejecución y

liquidación del contrato. En el evento en que el representante legal del oferente tenga límites por la naturaleza de los actos o de la cuantía, deberá aportar la respectiva autorización del órgano social correspondiente.

Con los términos de referencia definitivos serán exigidos los siguientes documentos:

- ii. El certificado de existencia y representación legal emitido por la Cámara de Comercio, con fecha de expedición no superior a treinta (30) días calendario anteriores a la fecha de presentación de la oferta.
- iii. Para empresas extranjeras sin sucursal en Colombia, se debe aportar el documento idóneo, expedido en el país de domicilio del oferente, que acredite la existencia de la sociedad, su objeto social, duración y representación legal. Tener en cuenta que los servicios que abarcan el objeto GRUPO, así como la forma de pago demanda representación en el territorio colombiano, por lo que el adjudicatario debe considerar que, es necesario registrar las copias auténticas de la fundación de la sociedad en la Cámara de Comercio de Colombia, para que sea establecida la sucursal.
- iv. Las autorizaciones del órgano social correspondiente, en los casos en los que el representante legal o apoderado tengan restricciones por la naturaleza de los actos o de la cuantía, o para el caso que así se requiera.

### 1.2.2. OFERTAS EN ASOCIACIÓN

ETB acepta la presentación de ofertas en asociación, caso en el cual deberá cumplir con los siguientes requisitos:

- Presentar documento que indique:
    - Integrantes de la asociación;
    - Tipo de Asociación;
    - Obligaciones y actividades a cargo de cada uno de los asociados en la ejecución del contrato, las cuales no podrán ser modificadas sin el consentimiento previo y escrito de ETB;
    - Porcentaje de participación el cual debe ser acorde con lo anterior y con el requisito del capítulo técnico;
    - Designación de la persona que para todos los efectos representará a la asociación, con facultades amplias y suficientes para obligar a todos sus integrantes en la presentación y negociación de la oferta, suscripción y ejecución del contrato, así como judicial y extrajudicialmente. El representante designado deberá manifestar su aceptación;
    - La duración de la asociación conformada o de la promesa de sociedad futura, deberá ser mínima por el lapso comprendido entre el recibo de ofertas del proceso de invitación y la liquidación del contrato. Lo anterior, sin perjuicio de que, con posterioridad, los integrantes de la asociación oferente estén llamados a responder por hechos u omisiones ocurridos durante la ejecución del contrato;
    - En todo caso, los asociados responden en forma solidaria frente a ETB por la presentación de la oferta, la suscripción del contrato y su ejecución;
- De conformidad con el literal anterior y atendiendo al régimen jurídico aplicable a ETB, las sanciones derivadas del incumplimiento de las obligaciones contenidas en la propuesta presentada por la unión temporal, consorcio o cualquier otra

asociación **no** se aplicarán en proporción al porcentaje de participación de cada uno de sus integrantes, como lo dispone la Ley 80 de 1993 para uniones temporales y consorcios, dado que dicha normatividad **no** es aplicable a ETB.

## LEGALIZACIÓN DE DOCUMENTOS EXPEDIDOS EN EL EXTERIOR.

Para el proceso de selección y una vez consolidados los términos de referencia definitivos, se debe tener en cuenta que, los documentos expedidos en el exterior deben ser presentados en idioma del país de origen, apostillados o legalizados y traducidos oficialmente al castellano conforme a lo dispuesto en la Resolución 1959 de 2020 y complementarias expedidas por el Ministerio de Relaciones Exteriores de Colombia.

Estos requisitos serán exigidos para que surtan efectos legales de validez y oponibilidad en Colombia de documentos expedidos en el exterior y que puedan obrar como prueba, conforme a lo dispuesto en el artículo 251 del Código General del Proceso, 480 del Código de Comercio.

### 1.2.3. ACREDITACIÓN DE REQUISITOS LEGALES EN SEGURIDAD SOCIAL Y SISTEMA DE GESTIÓN EN SEGURIDAD Y SALUD EN EL TRABAJO SG-SST (sociedades colombianas o sucursales de sociedades extranjeras).

Con los términos de referencia definitivos, será requerida la acreditación de la afiliación y el pago de los aportes a los sistemas de salud, riesgos laborales (ARL), pensiones (AFP), cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), cuando corresponda. Dicho cumplimiento deberá certificarse mediante documento expedido por el revisor fiscal, si lo hubiere, adjuntando copia de la cédula de ciudadanía, tarjeta profesional y certificación vigente de la Junta Central de Contadores, conforme a los requisitos legales. En caso de no contar con revisor fiscal, la certificación podrá ser emitida por el representante legal, de acuerdo con el artículo 50 de la Ley 789 de 2002. Adicionalmente, la acreditación de la implementación y cumplimiento de requisitos del sistema de gestión en seguridad y salud en el trabajo, Para tal efecto, el Oferente deberá aportar junto con la oferta la certificación emitida por la ARL donde conste el nivel de cumplimiento con un porcentaje mínimo del 85% del sistema, dicha certificación debe estar vigente en la fecha de su presentación, considerando la última modificación o actualización efectuada en la ARL.

### 1.2.4. ADJUDICACIÓN:

En la consolidación de los términos de referencia, ETB pretende celebrar los Acuerdo Marco, con quienes resulten habilitados con el cumplimiento de los requisitos mínimos habilitantes en los componentes jurídico, financiero y técnico.

ETB podrá abstenerse de adjudicar cuando el resultado del proceso no atienda los intereses de ETB. Los términos de referencia no constituirán jurídicamente una oferta de ETB dirigida a personas determinadas o indeterminadas, sino que constituyen invitaciones a los interesados a presentar ofertas a ETB. En ese sentido, por los términos de referencia, ETB no adquiere compromiso alguno de continuar con el procedimiento de contratación, ni de concluirlo mediante celebración de un contrato y podrá dar por terminado en cualquier momento el procedimiento de contratación sin aceptar oferta

alguna, y sin que haya lugar a reconocimiento económico alguno para los oferentes, quienes con la presentación de la oferta aceptan esta estipulación.

ETB podrá suspender o terminar, por decisión interna, el proceso de contratación en cualquiera de sus etapas cuando aparezcan circunstancias técnicas, operativas, económicas, de mercado, de fuerza mayor, orden de autoridad competente, acto irresistible de terceros o razones de utilidad o conveniencia corporativa, o cualquier otra que haga inconveniente la contratación. La decisión de suspensión o terminación del proceso será informada a los interesados o proponentes.

La adjudicación no supone derechos en cabeza del oferente y ETB no está obligada a suscribir un contrato; la adjudicación solo es el resultado de la evaluación de la oferta, cuyo proceso podrá ser declinado por ETB si así lo considera; o podrá continuarse mediante la firma de un contrato. Por tal razón, mientras que ETB no haya firmado un contrato, no se entiende que la oferta haya sido aceptada ni que se ha establecido una relación negocial o contractual con el adjudicatario, de la cual puedan derivarse obligaciones a cargo de ETB.

### 1.3. REQUERIMIENTO DE EJECUCIÓN, SEGUIMIENTO Y CONTROL

#### 1.3.1. PLAZO DE EJECUCIÓN DEL CONTRATO

El plazo de ejecución del contrato será de 2 años a partir de la orden escrita de inicio, previa aprobación de la garantía única de cumplimiento.

#### 1.3.2. GARANTÍAS CONTRACTUALES

El Acuerdo Marco exigirá una garantía de cumplimiento que el ALIADO debe constituir dentro de los 5 días hábiles siguientes a la fecha de suscripción del contrato, por un valor asegurado de \$200.000.000, vigente desde la fecha de suscripción del acuerdo marco, durante el plazo de ejecución y hasta la terminación.

Adicionalmente, dentro de los 5 días hábiles siguientes a la orden de servicios el Aliado Estratégico deberá constituir las garantías que sean exigidas de acuerdo con la naturaleza o alcance del servicio y será requisito para iniciar la ejecución del pedido contar con la aprobación de las pólizas.

**PARÁGRAFO:** Las garantías pueden ser expedidas a través del corredor de seguros de ETB o con cualquier compañía de seguros legalmente constituida en Colombia y Vigilada por la Superintendencia Financiera de Colombia.

##### 1.3.2.1. COBERTURAS DE LA GARANTÍA DE CUMPLIMIENTO.

**Se ampara el pago de multas y cláusula penal.**

El pago de multas corresponde a una sanción anticipada de perjuicios y la cláusula penal es la sanción por el incumplimiento total e irremediable del contrato.

**Retroactividad hasta 60 días.**

Emisión de pólizas sin carta de no reclamación con 60 días de retroactividad contados a partir del día de expedición de la póliza.

### **Prórroga automática hasta de 30 días.**

Período de tiempo durante el cual, aunque la aseguradora no tenga conocimiento de un documento que extienda el plazo contractual mientras que las partes surten el perfeccionamiento de este, se tendrá como prorrogado el amparo de cumplimiento por 30 días más.

### **Designación de ajustadores de común acuerdo (entre el beneficiario y la aseguradora)**

La designación del ajustador de siniestros debe efectuarse dentro de los tres (3) días siguientes a la fecha del aviso del siniestro, o a la fecha en que la empresa toma conocimiento de la ocurrencia. Cuando la empresa reciba el aviso de siniestro debe proponer al asegurado, por lo menos dos (2) días antes del vencimiento del plazo señalado, una terna de ajustadores de siniestros para que el asegurado manifieste su conformidad con la designación de alguno de los ajustadores propuestos. Para tal efecto, las empresas deben proponer a los ajustadores de siniestros que se encuentran inscritos y habilitados en el Registro correspondiente a cargo de la Superintendencia Financiera de Colombia. En caso de que el asegurado no designe alguno de los ajustadores de siniestros propuestos, la empresa procederá a designar el ajustador del siniestro antes del vencimiento del plazo señalado, a fin de no dilatar el estudio e inicio del proceso de liquidación del siniestro.

### **Ampliación aviso de siniestro a 30 días.**

En caso de reclamación se establece un plazo de 30 días para notificar a la aseguradora.

Toda solicitud de modificación deberá contar con el visto bueno de la ETB.

Para notificaciones o actualización de pólizas deberá existir un comunicado escrito por parte de ETB

### **1.3.2.2. COBERTURA DE LA GARANTÍA DE RESPONSABILIDAD CIVIL EXTRACONTRACTUAL.**

La garantía de Responsabilidad Civil Extracontractual derivada de cumplimiento deberá incluir al menos:

### **Designación de ajustadores de común acuerdo (entre el beneficiario y la aseguradora)**

La designación del ajustador de siniestros debe efectuarse dentro de los tres (3) días siguientes a la fecha del aviso del siniestro, o a la fecha en que la empresa toma conocimiento de la ocurrencia. Cuando la empresa reciba el aviso de siniestro debe proponer al asegurado, por lo menos dos (2) días antes del vencimiento del plazo

señalado, una terna de ajustadores de siniestros para que el asegurado manifieste su conformidad con la designación de alguno de los ajustadores propuestos. Para tal efecto, las empresas deben proponer a los ajustadores de siniestros que se encuentran inscritos y habilitados en el Registro correspondiente a cargo de la Superintendencia. En caso, el asegurado no designe alguno de los ajustadores de siniestros propuestos, la empresa procederá a designar el ajustador del siniestro antes del vencimiento del plazo señalado, a fin de no dilatar el inicio del proceso de liquidación del siniestro.

### **Ampliación plazo y revocación de la póliza.**

La Aseguradora podrá revocar o no prorrogar la póliza, mediante aviso previo al tomador de la póliza y a ETB, con un plazo no inferior a treinta (30) días.

### **Retroactividad hasta 60 días.**

Emisión de pólizas sin carta de no reclamación con 60 días de retroactividad contados a partir del día de expedición de la póliza.

### **Prórroga automática hasta de 30 días.**

Período de tiempo durante el cual, aunque la aseguradora no tenga conocimiento de un documento que extienda el plazo contractual mientras que las partes surten el perfeccionamiento de este, se tendrá como prorrogado el amparo de cumplimiento por 30 días más.

**1.3.3. MULTAS:** Como medida para apremiar al contratista a cumplir sus obligaciones contractuales ETB le podrá descontar hasta el 20% del precio de la orden de servicio y, establecerá en cada orden de servicio el valor o porcentaje aplicable por cada día de atraso o retardo en el cumplimiento de sus obligaciones, o por cualquier otra unidad de tiempo que se estime pertinente. El pago de la multa no exime al contratista del cumplimiento de la obligación contractual.

ETB podrá cobrar el valor de las multas mediante descuentos de las sumas de dinero que se adeuden al contratista por cualquier concepto. De no ser posible el descuento total o parcial, el contratista se obliga a consignar en la cuenta que ETB indique el valor o el saldo no descontado dentro del plazo que se señale en la cuenta de cobro que se le curse con tal fin. El contratista renuncia expresamente a todo requerimiento para efectos de su constitución en mora. El cobro de las multas garantizará el derecho al debido proceso del contratista.

### **1.3.4. CLÁUSULA PENAL**

El ACUERDO MARCO contemplará una cláusula penal pecuniaria de \$200.000.000, valor que armoniza con la garantía de cumplimiento la cual tiene como propósito respaldar las obligaciones diferentes a las de las órdenes de servicio ya que el Aliado asume la obligación de dar respuesta a las solicitudes de cotización que solicite ETB

Adicionalmente, en caso de incumplimiento definitivo de cualquiera de las obligaciones del Aliado, este se obliga a pagarle a ETB a título de cláusula penal el equivalente al 20% de la orden de servicio antes de IVA. La pena no exime al contratista del cumplimiento de la obligación principal ni del pago de los perjuicios que superen el valor de este porcentaje. El cobro de la cláusula penal respetará el derecho al debido proceso y la defensa del Aliado.

ETB podrá descontar el valor de la cláusula penal de las sumas que se adeuden al contratista por cualquier concepto. De no ser posible el descuento total o parcial, el contratista se obliga a consignar en la cuenta que ETB indique el valor o el saldo no descontado dentro del plazo que se señale en la cuenta de cobro que se le curse con tal fin. El contratista renuncia expresamente a todo requerimiento para efectos de su constitución en mora.

### 1.3.5. DECLARACIÓN JURAMENTADA.

No podrá participar en el proceso, ni celebrar contrato con ETB, las personas naturales o jurídicas que se encuentren incurso en alguna de las causales de inhabilidad o incompatibilidad. En consecuencia, al momento de presentar oferta el Aliado Estratégico debe declarar bajo la gravedad del juramento lo siguiente:

Que no se halla incurso en las causales de inhabilidad e incompatibilidad para contratar consagradas en la Constitución Política, y en las disposiciones legales contenidas en las Leyes 80 de 1993, 489 de 1998, 1150 de 2007, 1474 de 2011, 1801 de 2016, 1952 de 2019 reformada por la Ley 2094 de 2021, 1955 de 2019, 2014 de 2019, 2097 de 2021, 2195 de 2022, el Decreto 1082 de 2015, y demás normas que regulen las inhabilidades e incompatibilidades para contratar con el Estado. Así mismo declara que no se encuentra incurso en ninguna causal de conflicto de interés. Así mismo, se compromete a informar de manera inmediata por escrito a ETB cualquier situación sobreviniente que pueda constituir o generar conflicto de interés.

En caso de que el proponente presente oferta o celebre o ejecute el contrato encontrándose incurso en cualquiera de las situaciones descritas, deberá responder por los daños y perjuicios que cause a ETB o a terceros por su conducta.

### 1.3.6. COMPROMISO ANTICORRUPCIÓN

El Proveedor en calidad de Oferente o de Contratista, se compromete a:

- Cumplir todas las normas legales y éticas aplicables en materia de lucha contra la corrupción, incluyendo, pero sin limitarse las disposiciones contenidas en la Ley 1474 de 2011, la Ley 2195 de 2022 y demás normas concordantes nacionales e internacionales.
- Implementar controles razonables dentro de su organización para prevenir y detectar actos de corrupción, soborno o fraude. Estructurar propuestas serias, con información fidedigna y económicamente ajustadas a la realidad, que aseguren la ejecución del contrato en las condiciones de calidad y oportunidad exigidas en los términos de referencia.

- Actuar en el proceso de contratación con estricto apego a las normas jurídicas y éticas propias de este tipo de procedimientos, y conforme a los principios de buena fe, transparencia y equidad.
- No celebrar acuerdos ni incurrir en actos o conductas que tengan por objeto coludir en el proceso de selección.
- No interferir directa o indirectamente en la etapa de evaluación de las propuestas.
- A conocer y aplicar el código de ética de ETB.
- Denunciar cualquier acto, solicitud o insinuación de carácter corrupto, soborno o fraude en la presentación de la oferta y ejecución del contrato.

ETB promueve la actuación transparente de todos los intervinientes en sus procesos contractuales. En tal sentido, invita a los oferentes, contratistas y a la comunidad en general a reportar cualquier presunto hecho de corrupción, o posible violación o incumplimiento del Código de Ética y Conducta de ETB, a través de la Línea Ética (601) 242 2555 – 305 803 2842 o al correo electrónico [correo\\_etico@etb.com.co](mailto:correo_etico@etb.com.co).

### **1.3.7. COMPROMISO CON LA SOSTENIBILIDAD Y DESARROLLO DE BUENAS PRÁCTICAS DE RESPONSABILIDAD CORPORATIVA**

ETB extiende sus estándares de responsabilidad corporativa y sostenibilidad a sus contratistas, especialmente en materia de:

- a) Conducta ética.
- b) Protección de los derechos humanos.
- c) Buenas prácticas laborales.
- d) Transparencia, lucha contra la corrupción y el soborno.
- e) Rendición de cuentas para la construcción de relaciones de confianza con todos los grupos de interés del contratista, quien deberá tenerlos plenamente identificados.
- f) Protección del medio ambiente.
- g) Adopción de prácticas de responsabilidad social y sostenibilidad en la cadena de valor.

Por esta razón, ETB podrá solicitar en cualquier momento al CONTRATISTA aportar la información sobre la incorporación de estándares y herramientas de responsabilidad corporativa y sostenibilidad en la gestión de su empresa. Así mismo, ETB podrá solicitar en cualquier momento al CONTRATISTA su plan de sostenibilidad y responsabilidad corporativa en el marco del desarrollo del contrato.

Adicionalmente, al momento de ser requerido, el CONTRATISTA deberá entregar a ETB información sobre:

Promoción del respeto de los derechos humanos involucrando a todos sus grupos de Interés.

Buenas prácticas y cumplimiento de la normatividad laboral vigente en salud ocupacional, seguridad industrial y ergonomía, prohibición del trabajo infantil y la promoción de la diversidad, la equidad y la inclusión laboral, conforme a lo dispuesto en el aparte denominado “Exclusión de la Relación Laboral” de los términos de referencia.

Cumplimiento de la normatividad ambiental, protección del medio ambiente y respeto a las comunidades que hacen parte de su ámbito de influencia en el desarrollo de su actividad empresarial, conforme a lo dispuesto en el aparte denominado “Gestión Ambiental” de los términos de referencia.

Su compromiso con la transparencia, ética corporativa y lucha contra la corrupción y el soborno, conforme a lo dispuesto en el Anexo No. 1 “Carta de Presentación de la Oferta” y en el aparte denominado “Compromiso Anticorrupción” de los términos de referencia.

### **1.3.8. CUMPLIMIENTO DE REQUISITOS LEGALES EN SEGURIDAD SOCIAL, APORTES PARAFISCALES Y SISTEMA GENERAL DE SEGURIDAD EN EL TRABAJO SG-SST**

El contratista debe cumplir con los estándares mínimos de seguridad y salud en el trabajo (SG-SST), respecto a sus trabajadores y subcontratistas, acatando rigurosamente las obligaciones legales aplicables, en particular lo dispuesto en el Decreto 1072 de 2015, la Resolución 0312 de 2019 del Ministerio de Trabajo y las normas que las complementen o modifiquen.

El contratista está obligado a garantizar la afiliación y el pago de los aportes a los sistemas de salud, riesgos laborales (ARL), pensiones (AFP), cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar (ICBF) y Servicio Nacional de Aprendizaje (SENA), cuando corresponda. Dicho cumplimiento deberá certificarse mediante documento expedido por el revisor fiscal, si lo hubiere, adjuntando copia de la cédula de ciudadanía, tarjeta profesional y certificación vigente de la Junta Central de Contadores, conforme a los requisitos legales. En caso de no contar con revisor fiscal, la certificación podrá ser emitida por el representante legal, de acuerdo con el artículo 50 de la Ley 789 de 2002.

ETB podrá solicitar al contratista la entrega, digital, de las planillas de pago a las mencionadas entidades del personal vinculado para la ejecución del contrato, incluyendo subcontratistas. Asimismo, ETB podrá requerir certificaciones sobre el pago de obligaciones e indemnizaciones relacionadas con el personal que participe en la prestación del servicio, ya sea directamente o a través de subcontratistas, sin importar la modalidad de vinculación. Además, el contratista deberá garantizar la entrega de la dotación legal y de los elementos de protección personal (EPP) necesarios.

Sin perjuicio del cumplimiento de las demás obligaciones legales, el contratista deberá:

- a. Acreditar la implementación y cumplimiento del sistema de gestión en seguridad y salud en el trabajo, así como tener un responsable del sistema que cumpla con los requisitos establecidos por ley. Para tal efecto, el contratista debe aportar la certificación emitida por la ARL donde conste el nivel de cumplimiento con un porcentaje mínimo del 85% del sistema. Dicha certificación deberá ser presentada junto con la oferta y deberá encontrarse vigente en la fecha de su presentación, considerando la última modificación o actualización realizada por la ARL. Adicionalmente, para contratos superiores a un año de ejecución debe ser actualizada con una periodicidad anual y

aportada al supervisor del contrato.

- a. Garantizar que, en el marco de la autonomía técnica y administrativa, el personal a su cargo, (incluidos subcontratistas), esté debidamente capacitado, entrenado y con la inducción necesaria para ejecutar el contrato, incluyendo reinducción en seguridad y salud en el trabajo de ETB.
- b. Garantizar el entrenamiento y la capacitación para la ejecución de trabajos seguros, y contar con las certificaciones específicas y vigentes requeridas por la normativa aplicable, manteniéndolas disponibles para consulta.
- c. Entregar la dotación legal e industrial necesaria, así como los elementos de protección personal (EPP) para la ejecución de las actividades a cargo del contratista y subcontratistas, velando por su correcto uso.
- d. Cumplir las normas sobre prevención de riesgos laborales vigentes en Colombia, disponiendo de los recursos necesarios para la protección y prevención, garantizando la formación e información sobre los riesgos laborales de sus trabajadores (incluidos subcontratistas). El contratista y sus subcontratistas deberán velar por la seguridad del personal, asegurando el uso adecuado de los equipos de protección necesarios para el desarrollo de su trabajo, de conformidad con las normas legales.
- e. Garantizar un programa de capacitación en Seguridad y Salud en el Trabajo para sus trabajadores y subcontratistas, ejecutándolo durante la vigencia del contrato y conservando los soportes para su consulta de ETB en caso de ser requerido.
- f. Cumplir con lo establecido en el Programa de Seguridad y Salud en el Trabajo para contratistas de ETB, así como con las modificaciones o cambios que pudieran surgir, extendiendo su alcance a los subcontratistas. Para coordinar lo pertinente, el supervisor del contrato debe informar al área de Seguridad y Salud en el trabajo de ETB el nombre del contratista y el respectivo número de contrato.
- g. Suministrar durante la vigencia del contrato, y hasta 3 años después de la terminación o la liquidación cuando aplique, toda la información que ETB requiera sobre el cumplimiento de las obligaciones legales en materia de seguridad social, aportes parafiscales y SG-SST, incluso respecto a subcontratistas, sean personas naturales o jurídicas.

**Parágrafo primero:** Para acreditar el cumplimiento de los requisitos de los literales **b) al g)**, el representante legal del contratista debe emitir una certificación con una periodicidad anual, en la que conste que ha realizado la inducción, reinducción, capacitaciones y entrenamientos a sus trabajadores y subcontratistas. Asimismo, debe certificar que cumple con las normas sobre prevención de riesgos laborales, la entrega de dotación y elementos de protección personal, así como con lo establecido en el programa de seguridad y salud en el trabajo para contratistas de ETB.

**Parágrafo segundo:** El supervisor del contrato deberá remitir la información aportada por el contratista al equipo de Seguridad y Salud en el Trabajo de ETB para la revisión correspondiente, de acuerdo con el programa aplicable a contratistas. En todo caso, la interacción entre ETB y el Contratista será articulada por el supervisor del contrato.

### 1.3.9. PROPIEDAD INTELECTUAL

El Contratista deberá garantizar que la propiedad intelectual que aporte para la ejecución del contrato es de su titularidad o cuenta con las licencias necesarias para su uso, liberando a ETB de cualquier responsabilidad por posibles infracciones. En caso de reclamación de terceros, el Contratista asumirá íntegramente la responsabilidad legal y económica que se derive de dicha reclamación.

ETB y el Contratista se comprometen a respetar los derechos morales de autor establecidos en el artículo 11 de la Decisión Andina 351 de 1993 y en el artículo 30 de la Ley 23 de 1982.

Toda la información relativa a clientes, así como los datos conexos y la información que se genere en el marco de la ejecución del contrato, será de exclusiva propiedad de ETB.

### 1.3.10. SEGURIDAD DE LA INFORMACIÓN

Con la presentación de la oferta, se entiende que el oferente acepta, en caso de resultar adjudicatario, adherirse a las Políticas de Seguridad de la Información y Continuidad del Negocio adoptadas por ETB para la protección de su información y la de terceros. El proponente se compromete a conocer y cumplir dichas políticas, así como a instruir al personal que participe en la ejecución del contrato independientemente de su forma de vinculación sobre la obligatoriedad de su cumplimiento. Las políticas pueden consultarse en el sitio web de ETB: [www.etb.com](http://www.etb.com).

Los usuarios asignados al Contratista para acceder a los sistemas de información de ETB deben ser personas que efectivamente estén ejecutando actividades relacionadas con el objeto contractual. En este sentido, el Contratista se obliga a mantener informada a ETB sobre los usuarios bajo su responsabilidad que deben permanecer activos, notificando de manera inmediata cualquier retiro o cambio en el personal que acceda a dichos sistemas.

El Contratista acepta que ETB se reserva el derecho de negar o suspender el acceso a sus instalaciones físicas o sistemas de información a cualquier empleado directo o indirecto del Contratista, si considera que ha incurrido en actividades que contravengan las políticas de seguridad de la información, o que hayan sido dolosas o fraudulentas. ETB no estará obligada a presentar evidencias de tales hallazgos. No obstante, el Contratista se compromete a tomar las medidas necesarias para garantizar la continuidad de los servicios pactados con ETB. Asimismo, se obliga a prevenir que sus empleados directos o indirectos incurran en dichas conductas durante la ejecución de actividades relacionadas con el contrato. El Contratista acepta que ETB podrá monitorear en cualquier momento las actividades realizadas por sus empleados o subcontratistas en los sistemas de información de ETB.

El Contratista se compromete a reportar cualquier debilidad sospechosa que afecte la seguridad de la información, así como a informar de manera inmediata sobre incidentes que puedan comprometer la confidencialidad, integridad y/o disponibilidad de la información de ETB o de sus terceros. Además, deberá colaborar con todos los medios a su alcance para la remediación de dichos incidentes. Sin perjuicio de los reportes

realizados ante ETB, el Contratista será responsable por los perjuicios que se generen como consecuencia de incidentes que afecten la seguridad de la información y la continuidad del negocio.

El Contratista deberá impartir a su personal acciones de sensibilización, capacitación, entrenamiento y actualizaciones regulares en políticas y procedimientos de seguridad de la información y continuidad del negocio, según sea pertinente para la ejecución del contrato.

### 1.3.11. TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

Las Partes reconocen y aceptan que, en el desarrollo y ejecución del contrato, tendrán acceso a información que contiene datos personales, motivo por el cual deben dar cumplimiento en la medida en que aplique, a la normativa en la materia, en especial a, la Ley 1581 de 2012, la Ley 1266 de 2008, la Ley 2300 de 2023, el Decreto 1074 de 2015 y demás normas que las modifiquen, deroguen, adicionen o sustituyan (en adelante, la “Ley Aplicable”).

El CONTRATISTA acepta conocer y cumplir la Política de Tratamiento de Datos Personales de ETB vigente para, el tratamiento, transmisión o transferencia de información personal que gestiona incluyendo los datos de terceros. Así mismo, se obliga a instruir al personal que ocupe para la ejecución del contrato, independientemente de la forma de vinculación. La política puede ser consultada página WEB de ETB [https://etb.com/docs/Pol%C3%ADtica\\_tratamiento\\_datos\\_personales\\_ETB.pdf](https://etb.com/docs/Pol%C3%ADtica_tratamiento_datos_personales_ETB.pdf)

**Si en la ejecución del contrato se requiere realizar transmisión de datos personales al CONTRATISTA o el mismo trata datos personales a nombre de ETB, el CONTRATISTA se obliga a:**

- i. Realizar el Tratamiento de los Datos Personales en desarrollo del objeto del presente Contrato única y exclusivamente por cuenta de ETB como responsable del Tratamiento.
- ii. Abstenerse de realizar Tratamiento sobre los Datos Personales para fines distintos al cumplimiento del objeto y de las obligaciones del presente Contrato y de acuerdo con la finalidad que los Titulares hayan autorizado.
- iii. Garantizar la confidencialidad de la información que contenga datos personales, incluso después de la terminación del presente contrato.
- iv. Implementar medidas de seguridad técnicas, humanas y administrativas adecuadas para proteger los datos personales contra el acceso no autorizado, la adulteración, la pérdida, el daño, el uso o divulgación indebidos, o cualquier otra forma de tratamiento no autorizado o ilícito. Dichas medidas deben ser proporcionales a la naturaleza de los datos tratados y a los riesgos asociados a su tratamiento. El CONTRATISTA deberá documentar y mantener actualizadas dichas medidas.
- v. Realizar en el menor tiempo posible la actualización, rectificación o supresión de los datos en los términos establecidos en la Ley 1581 de 2012, lo establecido por ETB y cualquier norma que la reglamente, adicione o modifique.
- vi. No ceder, comunicar, transferir ni transmitir los datos personales a terceros, salvo que la Ley Aplicable lo permita o cuente con la autorización previa y expresa de

- ETB. En caso de contar con dicha autorización, el CONTRATISTA deberá asegurarse de que el tercero receptor cumpla con las mismas obligaciones de seguridad y confidencialidad estipuladas en el presente contrato.
- vii. Permitir el acceso a la información únicamente a las personas que deban tener acceso a ella para dar cumplimiento a las obligaciones del presente Contrato; bajo el entendido que las obligaciones de confidencialidad y Tratamiento de Datos Personales se extiendan a dichas personas y que el CONTRATISTA es garante del cumplimiento de dichas obligaciones.
  - viii. Actualizar la información reportada por ETB dentro de los tres (3) días hábiles contados a partir de su recibo, salvo que el marco normativo vigente establezca un plazo menor.
  - ix. Atender las consultas formuladas por ETB sobre el Tratamiento de Datos Personales efectuado por el CONTRATISTA dentro de los tres (3) días hábiles siguientes contados a partir de la fecha de recibo de la consulta salvo que el marco normativo vigente establezca un plazo menor.
  - x. Colaborar con ETB para garantizar el ejercicio de los derechos de los titulares de los datos (acceso, rectificación, supresión, revocación del consentimiento, entre otros), incluyendo la asistencia en la respuesta a solicitudes de los titulares.
  - xi. Notificar de forma inmediata a ETB al correo electrónico: [Unidad de Cumplimiento@etb.com.co](mailto:Unidad_de_Cumplimiento@etb.com.co), [oficialdatospersonales@etb.com.co](mailto:oficialdatospersonales@etb.com.co), cualquier violación de seguridad de los datos personales de la que tenga conocimiento, que pueda implicar un riesgo para los derechos y libertades de los titulares de los datos personales. Esta notificación deberá incluir toda la información relevante y disponible para ETB.
  - xii. Devolver a ETB y posteriormente destruir (eliminar) en caso de que aplique, todos los datos personales a los que haya tenido acceso o que haya tratado en virtud del presente contrato, una vez finalizado el plazo contractual o cuando ETB o el titular así lo solicite, salvo que exista un deber legal o contractual de conservar los datos personales. El CONTRATISTA deberá certificar por escrito la completa devolución y posterior destrucción de los datos personales. La supresión de cualquiera de los datos mencionados debe ser documentada mediante acta suscrita por el representante legal del CONTRATISTA y compartida a ETB.
  - xiii. Permitir y facilitar las auditorías e inspecciones que realice ETB o un tercero autorizado por esta, para verificar el cumplimiento de las obligaciones en materia de protección de datos personales establecidas en esta cláusula y en la Ley Aplicable.
  - xiv. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio sobre Tratamiento de Datos Personales.
  - xv. Mantener un registro de las actividades de tratamiento que realice en nombre de ETB, conforme lo exigido en la Ley Aplicable.

En caso de que, durante la ejecución del contrato, **se requiere realizar una transmisión internacional de datos personales**, el CONTRATISTA acepta dar cumplimiento a las disposiciones vigentes en materia de protección de datos personales sobre transferencia y transmisión internacional de datos personales.

**Si para la finalidad del cumplimiento del objeto del contrato ETB requiere realizar el tratamiento de datos personales del personal del CONTRATISTA, el CONTRATISTA declara que cuenta con la autorización de Tratamiento de Datos, para**

entregar los datos de contacto de su personal que estará encargado de todo o parte de la ejecución del presente Contrato, siempre que se requiera para la ejecución. Por lo tanto, autoriza a ETB para almacenar, recolectar, usar, transferir, transmitir, suprimir, verificar y procesar en sus Bases de Datos toda la información del personal del CONTRATISTA Involucrado para la correcta ejecución del Contrato, por lo cual el CONTRATISTA se obliga a transferir los Datos Personales de su personal involucrado siempre que se requiera para permitir la ejecución del presente Contrato.

**Indemnidad y Responsabilidad:** El CONTRATISTA será el único responsable y deberá indemnizar a ETB por cualquier daño, perjuicio, multa, sanción o reclamo (incluyendo honorarios de abogados y costos de defensa) que ETB deba asumir o pagar como consecuencia directa o indirecta del indebido tratamiento o por el incumplimiento por parte del CONTRATISTA de las obligaciones establecidas en la presente cláusula o en la Ley Aplicable.

En caso de que un titular de datos o una autoridad competente exija o inicie acciones contra ETB por un tratamiento de datos realizado por el CONTRATISTA en contravención de la presente cláusula, la Ley Aplicable y de la Política de Tratamiento de Datos de ETB, el CONTRATISTA se compromete a asistir a ETB en su defensa y a asumir los costos asociados a dicha defensa, así como las eventuales condenas o sanciones que se impongan a ETB.

### 1.3.12. GESTIÓN AMBIENTAL

El Contratista deberá ejecutar las obligaciones a su cargo en cumplimiento de las normas legales vigentes sobre gestión ambiental. Por lo anterior, le corresponde, entre otras obligaciones, realizar las actividades relativas a identificar, analizar y evaluar peligros, a controlar y gestionar riesgos, a mitigar, corregir o compensar los impactos y efectos ambientales que puedan afectar a las personas, propiedades o medio ambiente y obtener los permisos requeridos por las autoridades ambientales. Estas obligaciones se extienden a sus subcontratistas.

El contratista reconoce que la responsabilidad medioambiental es parte integral del desarrollo del objeto contratado, por lo que el contratista identificará las repercusiones medioambientales de las actividades a realizar para ejecutar el objeto contratado y minimizará los efectos adversos en la comunidad, en el medioambiente y en los recursos naturales, a la vez que proteja la salud y la seguridad pública en general.

Los estándares medioambientales son:

#### Cumplimiento de Normatividad Ambiental

El Contratista deberá ejecutar las obligaciones a su cargo en cumplimiento de las normas legales vigentes sobre gestión ambiental. Por lo anterior, le corresponde, entre otras obligaciones, realizar las actividades relativas a identificar, analizar y evaluar aspectos ambientales, a controlar y gestionar riesgos, a mitigar, corregir o compensar los impactos y efectos ambientales que puedan afectar a las personas, propiedades o medio ambiente. Estas obligaciones se extienden a sus subcontratistas.

Permisos e informes medioambientales

El contratista obtendrá todos los permisos ambientales, aprobaciones e inscripciones, requeridos por las autoridades ambientales, se renovarán y mantendrán en vigor y se seguirán sus requisitos operativos y de notificaciones que se requieran para ejecutar el objeto contratado.

#### Prevención de la contaminación y reducción de recursos

Siempre que se pueda en desarrollo del objeto contratado, las emisiones, vertimientos de contaminantes y la generación de desechos se deben minimizar o eliminar en el punto de origen, con técnicas como modificación de procesos, mantenimiento, uso de equipos para controlar la contaminación, o por otros medios. Se requiere buscar la conservación de los recursos naturales, como el agua, los combustibles fósiles, los minerales y los productos forestales, a través de sustitución de materiales, reutilización, conservación, reciclaje o por otros medios viables.

#### Sustancias peligrosas

En desarrollo del objeto contratado, el contratista garantizará que las sustancias químicas, residuos u otros materiales que supongan un peligro para las personas o para el medioambiente se identificarán, etiquetarán y gestionarán para garantizar que su manipulación, desplazamiento, almacenamiento, uso, reciclaje o reutilización y eliminación se haga de manera segura.

#### Desechos sólidos

En desarrollo del objeto contratado el contratista identificará, gestionará, reducirá y eliminará de forma responsable o reciclará los desechos sólidos peligrosos como no peligrosos, siempre que aplique.

#### Emisiones al aire

El contratista identificará y caracterizará, cuando aplique, las emisiones al aire de sustancias químicas orgánicas volátiles, aerosoles, corrosivos, partículas, sustancias que destruyen la capa de ozono y productos derivados de la combustión que se generen durante la ejecución del contrato.

Las sustancias que destruyen la capa de ozono deben gestionarse de forma eficaz de acuerdo con el Protocolo de Montreal y las normativas aplicables.

#### Restricciones de materiales

El contratista cumplirá las leyes, normativas y requisitos de los clientes relacionados con la ejecución del contrato; así mismo, incluirá la prohibición o restricción del uso de sustancias contaminantes en los productos y su fabricación cuando aplique. De la misma manera, deberá incorporar el respectivo etiquetado para su reciclaje o eliminación.

#### Gestión del agua

El contratista deberá implementar buenas prácticas en las que se controlen las fuentes de agua, su uso y su vertido, procurando oportunidades para conservar el agua y controlar los canales de contaminación. En caso de que aplique, las aguas residuales se caracterizarán, y se realizará el monitoreo, el control y el tratamiento requerido antes de su vertido o eliminación. En caso de que aplique el contratista deberá llevar a cabo un control periódico del rendimiento de los sistemas de tratamiento y contención de aguas residuales para garantizar un rendimiento óptimo, así como el cumplimiento normativo.

### Consumo energético

El contratista deberá buscar métodos rentables para mejorar la eficiencia energética y reducir el consumo energético y, a su vez, las emisiones de gases de efecto invernadero.

### 1.3.13. ADMINISTRACIÓN DEL RIESGO DE LAVADO DE ACTIVOS, FINANCIACIÓN DEL TERRORISMO Y FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA (LA/FT/FPADM)

El contratista declara que cumple con la normatividad colombiana vigente, incluyendo la implementación de un sistema de prevención del riesgo de lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva. Así mismo, se compromete a implementar buenas prácticas de debida diligencia en el conocimiento de sus contrapartes y en el monitoreo de sus actividades.

El contratista declara que ni él, ni sus representantes legales, socios, accionistas, administradores, clientes, empleados, revisores fiscales, contratistas y proveedores, se encuentran incluidos en listas restrictivas, ni han sido objeto de investigaciones o condenas por delitos relacionados con lavado de activos, financiación del terrorismo o corrupción. ETB puede verificar esta información y, en caso de identificar irregularidades, podrá dar por terminada la relación comercial de manera inmediata.

Igualmente, el contratista declara que no tiene presencia en países sancionados por la Oficina de Control de Activos Extranjeros (OFAC), y que su constitución no ha sido realizada bajo el esquema de acciones al portador. En caso de que el contratista tenga subcontratistas, estos deben cumplir con las mismas disposiciones establecidas en el presente documento.

El Contratista se compromete a actualizar su información, como mínimo una vez al año o cuando sea requerido por ETB, y a entregar cualquier información que sea relevante para la administración del riesgo de lavado de activos y financiación del terrorismo o de la proliferación de armas de destrucción masiva.

El contratista autoriza expresamente a ETB para comunicar a las autoridades competentes tanto nacionales como internacionales, cualquier situación descrita en el presente documento, así como a suministrar la información requerida. ETB podrá solicitar aclaraciones sobre las operaciones del contratista y, si no son satisfactorias, terminar la relación comercial.

El incumplimiento de las obligaciones aquí señaladas facultará a ETB para dar por terminada la relación contractual de manera inmediata, sin derecho a indemnización, y el contratista deberá responder por los perjuicios que se deriven de dicho incumplimiento.

### 1.3.14. EXCLUSIÓN DE LA RELACIÓN LABORAL

El presente contrato tiene naturaleza civil y no genera relación de carácter laboral. En consecuencia, el contratista actúa con plena autonomía técnica y administrativa, asumiendo independencia en la organización y dirección de sus actividades sin estar

sujeto a subordinación o dependencia de ETB. Por lo tanto, el contratista no recibirá instrucciones más allá de las especificaciones contractuales pactadas.

Todo el personal que intervenga en la ejecución del contrato será vinculado exclusivamente por el contratista, quien asumirá en forma integral las obligaciones laborales, de seguridad social, fiscales y parafiscales derivadas de dicha vinculación, sin que exista relación alguna entre el personal del contratista y ETB.

Cualquier vínculo laboral o contractual que el contratista adquiera con terceros será responsabilidad del contratista y, por tanto, ETB queda exonerada de cualquier obligación o reclamación derivada de dichos vínculos.

El contratista se obliga a emplear por su propia cuenta y riesgo, el personal, equipos, herramientas, materiales e insumos necesario para el cumplimiento de las obligaciones contractuales.

El contratista será responsable de coordinar y organizar libremente los medios necesarios para el desarrollo del contrato, sin perjuicio de la supervisión que pueda ejercer ETB para las verificaciones que correspondan

En el ejercicio de su autonomía técnica y administrativa, y bajo su propio riesgo, el Contratista es quien lleva a cabo el proceso de selección del personal con la experiencia necesaria para la ejecución del contrato. El Contratista se compromete a:

- Verificar y corroborar, mediante consultas o estudios de seguridad, la información judicial del personal que formará parte de su estructura, asegurando su idoneidad para la correcta ejecución.
- Cumplir con todas las disposiciones legales relacionadas con la modalidad de contratación del personal requerido para la prestación del servicio contratado, y garantizar el pago oportuno de todas las obligaciones derivadas de dicha contratación, conforme al marco legal vigente.
- En caso de vinculación de personal extranjero, el Contratista deberá dar cumplimiento a las normativas migratorias vigentes, así como obtener los permisos correspondientes para la contratación de dicho personal.
- Garantizar que no exista trabajo infantil en el marco de la ejecución del contrato. Además, el Contratista se compromete a no contratar personal a través de cooperativas de trabajo asociado, ni bajo la modalidad de aprendizaje.
- Garantizar que la contratación de su personal y la ejecución del contrato no afecten los derechos constitucionales, legales y laborales de los trabajadores.
- Asegurar que el salario o los pagos pactados con su personal estén en línea con el nivel de conocimiento y los requisitos de experiencia requeridos para la ejecución del contrato, respetando siempre los parámetros establecidos por la ley y las condiciones del mercado.
- Garantizar que la prestación de los servicios contratados no se vea afectada por altos índices de rotación del personal.
- Conceder al personal las licencias y permisos de ley, así como el disfrute de vacaciones, conforme lo estipula la ley, cuando haya lugar.
- Pagar la remuneración a pagar a su personal acorde a la experiencia y que no esté por debajo de los parámetros establecidos en la ley o en el mercado.

- Designar un delegado para la ejecución del contrato, quien será el encargado de interactuar con ETB en todos los asuntos laborales relacionados con el contrato. Además, liderará al personal del contratista, asegurando el adecuado desarrollo del contrato y la dirección administrativa.

### 1.3.15. CESIÓN DEL CONTRATO

El Contratista no podrá ceder su posición contractual, ni los derechos u obligaciones derivados del contrato, sin el consentimiento previo, expreso y por escrito de ETB. El cesionario deberá cumplir con los mismos requisitos de idoneidad, experiencia y capacidad exigidos al cedente.

Asimismo, el cesionario deberá presentar una declaración expresa en la que manifieste que la cesión no afectará el cumplimiento de las obligaciones contractuales.

La cesión solo tendrá efectos a partir de la firma del documento de autorización respectivo, suscrito por el cedente, el cesionario y ETB. En consecuencia, los pagos únicamente se efectuarán sobre las actividades ejecutadas por el cesionario con posterioridad a la firma del referido documento.

### 1.3.16. CESIÓN DE DERECHOS ECONÓMICOS:

En el evento de cesión de derechos económicos o diputación de pagos, el Contratista deberá informar mediante comunicación escrita al supervisor del contrato sobre el cesionario de los derechos económicos o allegar el poder general o especial para que el tercero reciba el pago, previa elaboración de documento por parte de ETB.

La suma por pagar debe haberse causado; para tal efecto, se tendrán en cuenta los descuentos a que haya lugar según lo contractualmente pactado, así como los embargos decretados por el juez conocidos por ETB al momento de autorizar y darse por entendida la notificación de los derechos económicos, o de efectuarse el pago al tercero, que para el caso de diputación corresponde al mandatario.

### 1.3.17. SUBCONTRATACIÓN

El Contratista únicamente podrá subcontratar con la autorización previa y expresa de ETB. La participación de subcontratistas no relevará al Contratista de su calidad de obligado frente a ETB ni lo eximirá del cumplimiento pleno de las obligaciones contractuales. En consecuencia, el Contratista seguirá siendo el único responsable ante ETB por la correcta ejecución del contrato.

ETB podrá exigir al Contratista, en cualquier momento, la terminación del subcontrato respectivo, así como el cumplimiento inmediato y directo de las obligaciones subcontratadas o el reemplazo del(los) subcontratista(s), cuando a su juicio, estos no cumplan con las calidades mínimas requeridas para la adecuada ejecución.

### 1.3.18. TERMINACIÓN DEL CONTRATO:

El contrato que llegue a suscribirse terminará por las causales legales o por las siguientes: (i) Por vencimiento del plazo. (ii) Por mutuo acuerdo. (iii) De manera anticipada por ETB, en cualquier momento, mediante aviso escrito al contratista con una antelación mínima de treinta (30) días calendario. (iv) Por incumplimiento de cualquiera de las prácticas establecidas en el apartado denominado “Compromiso con la sostenibilidad y el desarrollo de buenas prácticas de responsabilidad corporativa” de los presentes Términos de Referencia, por parte del contratista. (v) De manera anticipada por cualquiera de las partes en cualquier momento, cuando sean incluidos en listas restrictivas, vinculantes o no vinculantes, de carácter nacional o internacional. (Vi) Cuando el contratista incurra en cualquier causal de inhabilidad o incompatibilidad.

En ningún caso, la terminación anticipada del contrato dará lugar al reconocimiento de indemnización alguna por parte de ETB. En tales eventos, únicamente se reconocerán y pagarán al contratista las sumas correspondientes a los servicios solicitados y efectivamente entregados y recibidos a satisfacción.

### 1.3.19. SUPERVISIÓN

De conformidad con el Manual de Supervisión, se delega la supervisión así:

Durante la ejecución del contrato, ETB podrá realizar visitas a las instalaciones del CONTRATISTA, cuando lo considere necesario como parte de la gestión de supervisión y control a la correcta ejecución del contrato.

### 1.3.21. INDEMNIDAD

El Contratista se obliga a mantener indemne a ETB frente a cualquier reclamación, demanda o acción judicial o extrajudicial, multa, sanción o contingencia de cualquier índole, derivada de los actos, omisiones o negligencia del Contratista, su personal, subcontratistas o terceros relacionados con la ejecución del contrato.

En particular el contratista, asumirá directamente cualquier reclamación relacionada con:

- Obligaciones laborales, de seguridad social, parafiscales o de cualquier otra naturaleza frente al personal que emplee o contrate para la ejecución del contrato.
- Daños o perjuicios ocasionados a terceros o a bienes de ETB o de terceros, como consecuencia directa o indirecta de la ejecución del contrato.
- Incumplimientos normativos, técnicos, ambientales, de seguridad industrial o de cualquier otra regulación aplicable.
- El Contratista será el responsable exclusivo por todos los costos, gastos, honorarios legales y demás erogaciones que se causen con ocasión de las reclamaciones, sin perjuicio de las acciones legales que ETB pueda ejercer para el reconocimiento de perjuicios adicionales.

El contratista debe mantener indemne a ETB de toda reclamación o demanda, por los daños y perjuicios que ocasione el personal a su servicio a ETB o a terceros en desarrollo del contrato o por cualquier otro evento imputable a su responsabilidad.

### 1.3.22. ORDEN DE PRELACIÓN DE DOCUMENTOS CONTRACTUALES

Canales de radicación oficial:

Físico: Carrera 8 No 20 - 56 Piso 1 Ventanilla de Correspondencia

Digital: [gestioncorrespondencia@etb.com.co](mailto:gestioncorrespondencia@etb.com.co)



En caso de discrepancia o divergencia entre los documentos que hacen parte integral del contrato, prevalecerá su aplicación en el siguiente orden: i) Términos de Referencia, Anexos y Adendas; ii) Contrato y iii) Oferta del contratista.

### 1.3.23. SOLUCIÓN DE CONFLICTOS

Las controversias o diferencias que surjan entre las Partes con ocasión de la firma, ejecución, interpretación o terminación de los contratos suscritos y ejecutados en vigencia del presente Manual, así como cualquier otro asunto relacionado con los mismos, podrán ser sometidas a la revisión de las Partes para buscar un arreglo directo, en un término no mayor a treinta (30) días calendario contados a partir de la fecha en que cualquiera de las Partes comunique por escrito a la otra la existencia de una diferencia.

En caso de que las controversias o diferencias no sean resueltas de forma directa entre las partes, podrán acudir a mecanismos tales como la conciliación, transacción, amigable composición, entre otros mecanismos alternativos de solución de conflictos previstos en el ordenamiento jurídico vigente, previo cumplimiento de los requisitos que para el efecto disponga ETB.

Pese a lo indicado, en cualquier momento, las Partes podrán acudir a la jurisdicción competente para resolver los conflictos que se presenten.

07-07.7-F-025-v.7

01/08/2025

"Una vez impreso este documento, se considerará **documento no controlado**".

## CAPITULO II- CAPITULO FINANCIERO

Las siguientes son las condiciones financieras aplicables a la presente contratación, de conformidad con las especificaciones técnicas contenidas en el presente documento.

### 2.1 ESQUEMA DE COTIZACIÓN DE LOS PRECIOS

Para la cotización de precios del **ACUERDO MARCO**, ETB solicita que los servicios relacionados en los anexos financieros de cada grupo sean cotizados bajo el sistema de precios de referencia netos. Para efectos de este sistema, se entiende que el precio inicialmente cotizado por dichos servicios constituye el precio máximo que ETB reconocerá durante el plazo de ejecución del contrato.

Los precios máximos pactados servirán como base para que los Aliados presenten sus mejores descuentos en la cotización de cada orden de servicio que sea requerida por ETB, conforme al procedimiento establecido en el capítulo tercero del presente documento.

Serán por cuenta del proveedor y se considerarán incluidos como parte del precio, todos los impuestos, derechos, tasas y contribuciones de cualquier orden, vigentes en la fecha de suscripción del contrato. Si durante su ejecución los impuestos aumentan o se crean nuevos, serán asumidos por quien corresponda de acuerdo con la Ley; si disminuyen o se suprimen se pagará sobre lo efectivamente causado.

De todo pago o abono en cuenta que se efectúe, ETB hará las retenciones de ley a que haya lugar.

### 2.2. VALOR DE LA OFERTA

**El oferente deberá diligenciar y entregar los anexos definidos a continuación para este grupo a participar:**

#### **Grupo II Ciberseguridad**

**Anexo Financiero N° 1: Relación de precios Unitarios para los servicios de Ciberseguridad incluido IVA.**

**NOTA 1:** Los anexos de cotización deberán ser entregados en medio digital, en formato Excel, en archivos formulados.

**NOTA 2:** **El oferente deberá cotizar todos y cada uno de los precios unitarios** solicitados en los anexos de cotización solicitados en formato Excel de acuerdo al grupo o grupos que desean cotizar estos precios se ejecutarán por demanda de acuerdo con las necesidades puntuales en ejecución del contrato. La inobservancia a esta estipulación será causal de descarte de la oferta.

**NOTA 3:** El oferente deberá tener en cuenta que los ítems relacionados en el formato Excel se ejecutarán por demanda.

Canales de radicación oficial:

Físico: Carrera 8 No 20 - 56 Piso 1 Ventanilla de Correspondencia

Digital: [gestioncorrespondencia@etb.com.co](mailto:gestioncorrespondencia@etb.com.co)



**NOTA 4:** El oferente no podrá modificar los precios unitarios cotizados en los anexos remitidos en formato Excel, como consecuencia de las solicitudes de aclaración que ETB le formule. El incumplimiento a esta estipulación será causal de rechazo de la oferta.

**NOTA 5: El no diligenciamiento de al menos un ítem de un anexo financiero de cualquier grupo dará lugar a la descalificación de su oferta.**

**NOTA 6:** Entendemos que la información entregada en los anexos remitidos en formato Excel, está avalada y aprobada en su totalidad por el representante legal de la Cia.

El presente contrato se ejecutará mediante “órdenes de servicio” las cuales se realizarán según los parámetros y metodologías, lineamientos establecidos y definidos en el capítulo técnico de los presentes términos de referencia y según aplique para una u otra necesidad de la compañía.

El valor de la oferta para cada pedido se establecerá según cotización solicitada a LOS CONTRATISTAS, que queden seleccionados para la línea de servicio objeto de la presente contratación.

## 2.3 CUBRIMIENTO DE LA OFERTA

El precio de cada ítem "servicio" a cotizar debe incluir todos los bienes y servicios requeridos para cumplir a cabalidad con el objeto y alcance de la presente invitación. Cualquier elemento, unidad, módulo o material que se requiera para el cumplimiento del objeto contractual y que no haya sido incluido en la propuesta deberá ser suministrado en su totalidad por el posible CONTRATISTA sin costo adicional alguno para ETB, respecto del precio unitario cotizado negociado y contratado

Todos los costos, gastos, honorarios y demás egresos que sean necesarios para el cumplimiento de las obligaciones por parte del contratista, deberán quedar incluidos en su oferta económica, previo análisis que efectúe el oferente por su cuenta y riesgo, de manera que aquellos costos, gastos, honorarios y demás egresos no previstos en la oferta, no serán asumidos por ETB, ni cargados a ésta de forma alguna.

## 2.4 CONDICIONES GENERALES

Las siguientes son las condiciones financieras generales de la presente invitación para todos los grupos:

- h) Los servicios objeto de la presente invitación deberán cotizarse obligatoriamente en pesos colombianos, en números enteros, es decir sin incluir decimales. En todo caso, ETB se reserva el derecho de redondear a cero decimales las cifras cotizadas en pesos colombianos, para lo cual utilizará la herramienta redondear de Excel.

## 2.5 FORMA DE PAGO DE LOS SERVICIOS

### 2.5.1 Grupo II Ciberseguridad

#### 2.5.1.1 Servicios Integral por Hora

07-07.7-F-025-v.7

01/08/2025

"Una vez impreso este documento, se considerará **documento no controlado**".

El cien por ciento (100%) del precio de los servicios por hora, se pagará mediante cortes mensuales vencidos sobre la cantidad horas solicitados y efectivamente prestados en el respectivo mes, a los noventa (90) días calendario siguientes a la radicación de la factura comercial en el portal de recepción de facturas de Cuentas por pagar de ETB, acompañada del Acta de recibo mensual a satisfacción de los servicios, la cual debe presentarse debidamente suscrita por el supervisor del contrato en ETB y el contratista.

### **2.5.1.2 Servicios Integral a todo costo mensual**

El cien por ciento (100%) del precio de los servicios, se pagará en pesos colombianos por mensualidades fijas vencidas, a los noventa (90) días calendario siguientes a la radicación de la factura comercial en el portal de recepción de facturas de Cuentas por pagar de ETB, acompañada del Acta de recibo mensual a satisfacción de los servicios, la cual debe presentarse debidamente suscrita por el supervisor del contrato en ETB y el contratista.

Los servicios se liquidarán por mes o fracción, de acuerdo con la prestación efectiva del servicio, por lo anterior los períodos inferiores a un mes se liquidarán de manera proporcional al precio mensual cotizado. Entendiendo que cada mes corresponde a 30 días.

### **2.5.1.3 Servicio de licenciamiento por Usuario por mes**

El cien por ciento (100%) del precio de los servicios de licenciamiento por usuario por mes, se pagará en pesos colombianos por mensualidades vencidas, sobre la cantidad de usuarios efectivamente solicitados en el mes, a los noventa (90) días calendario siguientes a la radicación de la factura comercial en el portal de recepción de facturas de Cuentas por pagar de ETB, acompañada del Acta de recibo mensual a satisfacción de los servicios, la cual debe presentarse debidamente suscrita por el supervisor del contrato en ETB y el contratista.

Los servicios se liquidarán por mes o fracción, de acuerdo con la prestación efectiva del servicio, por lo anterior los períodos inferiores a un mes se liquidarán de manera proporcional al precio mensual cotizado. Entendiendo que cada mes corresponde a 30 días.

**La facturación y pago de los servicios relacionados en los numerales 2.5.1.1, 2.5.1.2 y 2.5.1.3 se realizará de la siguiente manera conforme al hito de pago relacionado en cada uno de ellos:**

- **El contratista realizará la facturación de los servicios una vez sean aprobados a satisfacción por parte del Cliente.**
- **ETB realizará el pago de las facturas previamente radicadas, a los 90 días calendario, para que ETB realice el respectivo pago se requiere que el cliente de ETB previamente haya pagado efectivamente el valor de los servicios, previa conciliación realizada entre ETB y su contratista, acompañada del acta de recibo a satisfacción de los respectivos servicios, la cual deberá estar suscrita por el Supervisor del contrato y el contratista. Se entiende por pago efectivo el ingreso de los recursos a las cuentas de ETB.**

**En caso de que la factura sea rechazada por incumplimiento de requisitos legales, falta de soportes o cualquier otra causa justificada, de acuerdo con los términos de**

referencia sobre factura electrónica, el contratista deberá corregir las inconsistencias y radicar una nueva factura. En tal evento, el término de noventa (90) días calendario para el pago comenzará a contarse nuevamente desde la fecha de radicación de la nueva factura corregida.

Es importante que el oferente tenga en cuenta que en cada orden de pedido y/o servicio se confirmará las condiciones de pago correspondiente. No obstante, cuando la necesidad esté destinada a ETB, el oferente deberá tener en cuenta que el plazo de pago aplicable será de ciento veinte (120) días calendario.

### **PLAZOS JUSTOS (Aplica para todas las formas de pago)**

En cumplimiento de lo dispuesto en la Ley 2024 de 2020, ETB pagará las facturas de los servicios objeto de la presente contratación, conforme a lo establecido anteriormente, a los cuarenta y cinco (45) días calendario siguientes a la radicación de las facturas, en el portal de recepción de facturas de Cuentas por Pagar de ETB, junto con el Acta de recibo a satisfacción de los bienes y servicios correspondiente, a todas aquellas empresas cuyo tamaño empresarial corresponda a una micro, pequeña o mediana empresa.

En caso de que la factura sea rechazada por incumplimiento de requisitos legales, falta de soportes o cualquier otra causa justificada, de acuerdo con los términos de referencia sobre factura electrónica, el contratista deberá corregir las inconsistencias y radicar una nueva factura. En tal evento, se interrumpirá el cómputo del plazo de 45 días calendario, el cual se continuará calculando a partir del día siguiente en que el contratista realice los ajustes o subsanación solicitada en el documento.

El oferente deberá junto con la oferta económica debe acreditar su tamaño empresarial mediante la presentación de los siguientes documentos:

- Certificado de Existencia y Representación Legal expedido por Cámara de Comercio con fecha de expedición no mayor a 30 días calendario anteriores a la fecha límite de presentación de ofertas.

### **2.6 ABONO DE PAGO A CONTRATISTAS**

El Contratista deberá establecer el número de cuenta, modalidad de ésta (ahorro o corriente), y entidad financiera a la que deben abonarse los pagos. Así mismo, en el evento de cambio de la cuenta, el contratista deberá informar de inmediato y por escrito a la supervisión del contrato, quien a su vez deberá revisar y dar estricto cumplimiento a lo dispuesto en la Directiva Interna número 00674 **“Mediante la cual se establece el procedimiento para la gestión de información relacionada con la administración de datos básicos referentes a cuentas bancarias, cambio de destinatarios de los pagos de los proveedores y acreedores creados en el sistema SAP”** del 25 de febrero de 2019; la cual regula el tema.

### **2.7 REINTEGRO DE DINEROS POR PARTE DE LOS CONTRATISTAS CUANDO SE IDENTIFIQUEN MAYORES VALORES ENTREGADOS POR CUALQUIER CONCEPTO**

Cuando se identifiquen mayores valores entregados por cualquier concepto, éstos deben ser desagregados y reintegrados a ETB; para tal efecto, se emitirá una cuenta de cobro por la Dirección de Facturación y Cartera, con visto bueno del supervisor, previa liquidación e indexación por parte del Equipo de Apoyo financiero a la contratación de la Dirección de Abastecimiento.

Para efectos de la liquidación e indexación mencionada anteriormente, el supervisor del contrato deberá cursar solicitud al Equipo de Apoyo financiero al a contratación de la Dirección de Abastecimiento, en la cual deberá detallar toda la información requerida para el cálculo, esto es: el mayor valor pagado, la fecha real de pago, la fecha probable de devolución de los dineros por parte del contratista y demás información relevante para el cálculo.

El pago de estos valores será descontado de las sumas que se adeuden al contratista por cualquier concepto; en caso de no adeudar dineros al contratista o que estos sean insuficientes para el respectivo pago, el contratista deberá consignar dichos valores dentro del plazo establecido.

La metodología de indexación a aplicar es la siguiente:

- xvi. Se determinará la fecha en que se efectuó el respectivo pago.
- xvii. Se determinará el mayor monto pagado en pesos colombianos.
- xviii. Se determinará la fecha de devolución por parte del contratista.
- xix. Se indexará el monto en pesos entre la fecha en que se efectuó el respectivo pago y la fecha de devolución, utilizando los índices de precios al consumidor en el ámbito nacional, para la República de Colombia certificados por el DANE para dicho período. En caso de no contar con la inflación correspondiente al período a actualizar se tomará el promedio mensual o diario corrido del año, según sea el caso, y se hará el cálculo con base en ésta. Para el caso de enero, por no tener información que permita establecer el promedio, se tomará la del mismo período del año inmediatamente anterior. Para este cálculo se incluye el valor del IVA correspondiente.
- xx. En el evento en que el contratista no efectúe el reintegro en la fecha fijada para el efecto, ETB aplicará intereses de mora liquidados a la tasa máxima de interés de mora certificada por la Superintendencia Financiera de Colombia vigente entre la fecha fijada para la devolución de los dineros y la fecha real de pago.

## 2.8 VERIFICACIÓN DE LAS VENTAS FRENTE AL VALOR A CONTRATAR

Las ventas reportadas por el oferente nacional o extranjero en sus estados financieros en el último año fiscal (2024) **NO** podrán ser inferiores a DIEZ MIL TRESCIENTOS TRES (10.303) SMMLV.

**En todo caso, durante la ejecución del contrato, ninguna orden de pedido y/o de servicio podrá superar el monto de las ventas reportadas por el CONTRATISTA del año inmediatamente anterior a la fecha de su solicitud.**

- Para las ofertas presentadas en consorcio, unión temporal o cualquier otra forma de asociación, para obtener el valor de las ventas, con el cual se verifique la condición se seguirá el procedimiento descrito a continuación:
  - i) En el momento de presentación de la oferta el documento consorcial debe indicar el porcentaje de participación de cada uno de los integrantes, con lo cual se procederá a realizar el siguiente cálculo: **Porcentaje de participación dentro del grupo asociado por las ventas, para cada uno de los integrantes del grupo asociado.** La suma de estos valores corresponderá al valor de las ventas del grupo consorciado.

**Nota:** Para efectos de validar este requerimiento el oferente deberá adjuntar con el paquete financiero de la oferta, el Estado de Resultados del último año fiscal (**2024**), debidamente suscrito por contador público, revisor fiscal o quien haga sus veces, de conformidad con la legislación aplicable para el efecto.

### Ejemplo:

Consortio A&B; Participación A= 40% y B=60%; Ventas de A= \$100, Ventas de B=\$200. Ventas del consorcio para revisión del requisito habilitante Ventas A&B = ((100\*40%) +(200\*60%)) = \$160; este es el valor ponderado de ventas para este consorcio.

**LA CONDICIÓN PREVISTA EN EL ANTERIOR NUMERAL CONSTITUYE UN REQUISITO HABILITANTE DE NATURALEZA FINANCIERA PARA PARTICIPAR EN EL PRESENTE PROCESO DE INVITACIÓN PÚBLICA. LOS OFERENTES QUE NO CUMPLAN CON EL REQUISITO HABILITANTE FINANCIERO REFERIDO EN EL PRESENTE NUMERAL, SERÁN DESCALIFICADOS.**

## 2.9 HOMOLOGACIÓN DE OFERENTES

Los oferentes internacionales y nacionales, personas jurídicas y personas naturales, interesados en presentar oferta deberán estar homologados, de conformidad con los requisitos establecidos en las Políticas Financieras Generales de Contratación, documento que se encuentra publicado en la página web de ETB [www.etb.com.co](http://www.etb.com.co), excepto en aquellos casos que tales políticas así lo determinen.

La homologación debe estar actualizada con los estados financieros de la última vigencia fiscal y es un requisito adicional al registro en la base de datos de proveedores. Este proceso es administrado por la Dirección de Abastecimiento.

## 2.10. IMPUESTOS Y FACTURACIÓN

### 2.10.1 IMPUESTO SOBRE LAS VENTAS

Para la aplicación del Impuesto Sobre las Ventas, el oferente debe efectuar el hecho generador estipulado en el artículo 420 del Estatuto Tributario y discriminar con exactitud el precio correspondiente de los bienes y servicios objeto de la oferta y el valor del impuesto sobre las ventas que afecte la misma, indicando la base sobre la cual se liquida de acuerdo con las normas vigentes en la fecha de presentación de la oferta. En el evento

en que el oferente no discrimine el IVA y se cause dicho impuesto, ETB lo considerará incluido en el valor de los bienes y servicios relacionados en la oferta.

En la cláusula de precio del contrato se deberán discriminar los conceptos que lo conforman y el IVA, si éste se causa.

En ningún caso la base gravable del impuesto sobre las ventas podrá ser inferior al valor comercial de los bienes o de los servicios, según lo establecido en el artículo 463 del Estatuto Tributario.

En caso de que el servicio o bien suministrado sea de cuantía indeterminada o no tenga valor, el proveedor deberá responder por el reconocimiento de sus ingresos e impuestos según las normas tributarias vigentes.

Para efectos del impuesto sobre las ventas, los servicios prestados y los intangibles adquiridos o licenciados desde el exterior se entenderán prestados, licenciados o adquiridos en el territorio nacional y causarán el respectivo impuesto cuando el usuario directo o destinatario de los mismos tenga su residencia fiscal, domicilio, establecimiento permanente, o la sede de su actividad económica en el territorio nacional, de conformidad con el parágrafo 2 del artículo 420 del Estatuto Tributario.

## **2.10.2 RETENCIÓN A TÍTULO DE IVA EN CONTRATOS QUE INVOLUCREN PRESTACIÓN DE SERVICIOS EN EL TERRITORIO NACIONAL O DESDE EL EXTERIOR CELEBRADOS CON NO RESIDENTES NI DOMICILIADOS EN COLOMBIA**

Para efectos de lo dispuesto en el numeral 3º del artículo 437-2 del Estatuto Tributario, en el contrato respectivo se deberá discriminar el valor del impuesto sobre las ventas generado, que será objeto de retención por parte de ETB. El contrato servirá como soporte para todos los efectos tributarios.

## **2.10.3 RETENCIÓN EN LA FUENTE A TÍTULO DE IMPUESTO SOBRE LA RENTA E IVA APLICABLE A OFERENTES NACIONALES**

El porcentaje de retención a título de Impuesto sobre la Renta e IVA, se determinará de conformidad con la normatividad vigente, habiéndose establecido previamente, si el contratista es declarante o no del impuesto sobre la renta, si es gran Contribuyente o Autorretenedor y el régimen de impuesto a las ventas al cual pertenece (responsable o no responsable) o si vende o presta servicios excluidos del IVA. Para efectos de la retención de renta se aplicará el criterio de retención por servicios del 4% o 6% solo cuando el servicio contratado obedezca a acciones simples que requieran poco o nada de componente intelectual, en los demás casos se aplicará el criterio de la DIAN bajo el cual, independientemente de que se llame servicio para efectos de retención se clasificara como honorario del 10% o 11% ya que por su naturaleza y componente intelectual desborda la definición de servicio.

## **2.10.4 RETENCIÓN EN LA FUENTE, OFERENTES NO RESIDENTES NI DOMICILIADOS EN COLOMBIA**

### **2.10.4.1 A TÍTULO DE IMPUESTO SOBRE LA RENTA**

El porcentaje de retención a título de Impuesto sobre la renta se determinará al momento en el cual se efectúe el correspondiente pago o abono en cuenta, de acuerdo con las normas tributarias vigentes para pagos al exterior.

#### **2.10.4.2 A TÍTULO DE IMPUESTO SOBRE LAS VENTAS**

El porcentaje de retención a título de Impuesto sobre las ventas será equivalente al ciento por ciento (100%) del valor del impuesto de acuerdo con lo estipulado en el parágrafo 1º del artículo 437-1.

#### **2.10.5 RETENCIÓN EN LA FUENTE A TÍTULO DE IMPUESTO DE INDUSTRIA Y COMERCIO**

##### **2.10.5.1 OFERENTE PROVEEDOR NACIONAL**

El contratista deberá informar el régimen del impuesto de industria y comercio al cual pertenece (responsable o no responsable), la actividad económica y la tarifa del impuesto de industria y comercio en Bogotá, D.C., o en las ciudades del país que le corresponda. En caso de no informarla, le será asignada la tarifa de retención más alta, la cual se aplicará al momento que se efectúe el correspondiente pago o abono en cuenta. En este orden de ideas el contratista deberá informar los valores y lugares de las actividades gravadas realizadas en desarrollo del contrato.

##### **2.10.5.2 PROVEEDOR NO RESIDENTE NI DOMICILIADO EN EL PAÍS**

Sobre la enajenación en Colombia de bienes importados y los servicios prestados intermediarios o terceros en el territorio nacional, ETB practicará las retenciones en la fuente a que haya lugar de acuerdo con las normas tributarias municipales respectivas.

##### **2.10.6 RETENCIÓN A TÍTULO DE IMPUESTO DE TIMBRE**

A partir de lo dispuesto en el artículo 519 del Estatuto Tributario, cuando el acto o contrato supere las 6.000 UVT, el proveedor deberá pagar a ETB el impuesto de timbre. De conformidad con el parágrafo 2º del citado artículo, modificado por el Decreto 175 de 2025, a partir de 22 de febrero de 2025 la tarifa aplicable por concepto del impuesto de timbre es del 1%. Este impuesto deberá ser asumido por el CONTRATISTA en un porcentaje correspondiente al 50%, toda vez que ETB se encuentra exenta del pago, de acuerdo con lo establecido en los artículos 532 y 533, en concordancia con la Sentencia C-736 de 2007 proferida por la Corte Constitucional.

En armonía con lo anterior, se debe tener en cuenta que el pago del impuesto por parte del proveedor constituye un requisito previo al inicio del contrato y/o de la modificación del mismo, teniendo en cuenta que se trata de un impuesto de naturaleza especial, caracterizado por ser un tributo documental de causación instantánea, su recaudo no está sujeto a la emisión o no de una factura:

Por lo anterior, para actos o contratos nuevos de cuantía determinada, el recaudo debe efectuarse de manera inmediata o hasta el plazo establecido en la cuenta de cobro, y con anterioridad a la emisión de la orden de inicio por parte de ETB, por lo que el contratista

deberá consignar a ETB el valor correspondiente, en su calidad de entidad pública y agente retenedor, de conformidad con lo establecido en el artículo 1.4.1.2.10 del Decreto Único Reglamentario (DUR),

Las modificaciones de actos o contratos de cuantía determinada, el recaudo debe efectuarse de manera inmediata o hasta el plazo establecido en la cuenta de cobro, por lo que el contratista deberá consignar a ETB el valor correspondiente, en su calidad de entidad pública y agente retenedor, de conformidad con lo establecido en el artículo 1.4.1.2.10 del Decreto Único Reglamentario (DUR).

En el caso de los actos o contratos nuevos y modificaciones de cuantía indeterminada, de conformidad con el inciso 5 del artículo 519 del Estatuto Tributario, el recaudo se hará sobre cada pago o abono en cuenta al proveedor. (descuento en cada factura o cuenta de cobro tomando como base el valor de la factura antes de IVA)

Así las cosas, en la cuenta de cobro correspondiente se indicará la respectiva cuenta bancaria de recaudo del impuesto, valora pagar y el plazo. El contratista deberá remitir copia de la consignación al correo electrónico [recaudo@etb.com.co](mailto:recaudo@etb.com.co) con copia al supervisor del contrato o área contratante.

## 2.10.7 RÉGIMEN SIMPLE DE TRIBUTACIÓN

Si el oferente se ha acogido al régimen SIMPLE establecido para el año 2019, no se le debe aplicar la retención a título de Renta e ICA de conformidad con el artículo 911 del E.T. y el Decreto 1468 del 2019 respectivamente. Por consiguiente, solo se le aplicara la retención de IVA.

## 2.10.8 IMPUESTOS Y FACTURACIÓN A SUCURSAL EXTRANJERA

Si la oferta es presentada por un proveedor extranjero que cuenta con una sucursal constituida en Colombia a través de la cual realizará algunas o todas las actividades tendientes a cubrir el objeto de la presente contratación, deberá especificar en su oferta cuales serán estas labores y el valor correspondiente. Es de anotar que el valor de las actividades desarrolladas por la sucursal no será girado al exterior y debe ser facturado directamente por la sucursal, para lo cual se observarán las condiciones determinadas para la forma de pago para proveedor nacional.

Adicionalmente, para cotizar las actividades a desarrollar por la Sucursal deberá utilizar los anexos financieros correspondientes a nacionales.

## 2.10.9 FACTURACIÓN PARA CONTRATISTAS EN CONSORCIO, UNIÓN TEMPORAL O CUALQUIER FORMA DE ASOCIACIÓN

En el evento en que la oferta sea presentada bajo la modalidad de consorcio, unión temporal o cualquier forma de asociación, la facturación debe ajustarse a lo establecido en el artículo 1.6.1.4.10 del Decreto 1625 de 2016 – Decreto Único en Materia Tributaria, la cual permite que los consorcios o uniones temporales puedan facturar **“a nombre propio y en representación de sus miembros, o en forma separada o conjunta cada uno de los miembros del consorcio o unión temporal”** lo que dependerá de la forma en

que se ejecuten las actividades. Es decir, si quien presta el servicio o vende el bien es la Unión Temporal o Consorcio, es este quien debe expedir la respectiva factura. Por su parte, si quien vende el bien o presta el servicio es cada uno de los miembros en forma separada, cada uno de ellos deberá facturar la respectiva operación y si lo hacen en forma conjunta, así mismo, en conjunto, deberán expedir la respectiva factura.

## 2.10.10 RÉGIMEN TRIBUTARIO DE E.T.B.

ETB es Gran Contribuyente (Resolución 200 del 27 de diciembre de 2024), Autorretenedor de ingresos gravados con impuesto de renta (Decreto 2885 del 24 de diciembre de 2001, Resolución DIAN No. 0547 del 25 de Enero de 2002), Autorretenedor de rendimientos financieros (Resolución 2863 de 2018), responsable del Impuesto sobre las Ventas (artículo 792 del E.T.), catalogada como Entidad de Derecho Público para efectos de la retención por concepto de ICA para la ciudad de Bogotá, D. C. (Artículo 3 Decreto No. 271 del 28 de Junio de 2002). Código CIU 6110.

## 2.10.11 REQUISITOS EN LA FACTURACIÓN

El proveedor estará obligado a informar al momento de la facturación el régimen de impuesto sobre las ventas al cual pertenece si es responsable del impuesto o no, si los servicios que presta se encuentran excluidos del IVA y si es declarante o no del Impuesto sobre la Renta, si es gran contribuyente o autorretenedor de Renta y las disposiciones que lo autorizan. Así mismo deberá discriminar en que municipio presta el servicio.

Si el proveedor factura a través de apoderado, el documento deberá expresar que se expide por cuenta y a nombre del poderdante.

De igual manera se deberá discriminar en la factura el concepto de la comercialización de los productos y servicios, detallando si se tratan de actividades comerciales, o cualquier otra asociada.

De acuerdo con el artículo 66 de la Resolución 165 de 2023, que desarrolla los sistemas de facturación vigentes, establece el idioma y moneda en el contenido de los sistemas de facturación de venta, señalando: **“Se debe utilizar el idioma español y el peso colombiano en la generación de los sistemas de facturación,** sin perjuicio que además de expresar el respectivo valor en pesos colombianos pueda expresarse en otra moneda y en un idioma distinto al español.”

Para efectos del cumplimiento de los requisitos legales y de tomar como deducción los costos y gastos derivados de esta contratación, así como los impuestos descontables, es importante que en todos los casos en donde el pago de los bienes y servicios no se pague de contado, la factura debe indicar pago a crédito al igual que el archivo XML generado a la DIAN, esto de acuerdo con lo estipulado en el inciso 10 del artículo 616-1 del Estatuto Tributario, y el artículo 34 de la Resolución 85 de 2022 expedida por la DIAN.

## 2.10.12 RESPONSABILIDAD DEL PROVEEDOR O AGENTE SOBRE LOS TRIBUTOS

Es responsabilidad del proveedor o agente la correcta aplicación de los impuestos relacionados en la factura de venta, así como el cumplimiento de los requisitos de factura

o documento o equivalente según sea el caso. Los casos o situaciones no contempladas en estos términos ya sea por situaciones particulares, especiales o por desconocimiento de factores inherentes a la operación a realizar no desvirtúan en ningún caso la responsabilidad del proveedor o agente de aplicar correctamente los impuestos.

### 2.10.13 RADICACIÓN FACTURA ELECTRÓNICA

Para los pagos que **ETB** hará **al Proveedor** en virtud del presente contrato, se atenderá lo definido por la Resolución DIAN 165 del 1 de noviembre de 2023, Anexo Técnico, de la mencionada Resolución, facturación Electrónica Versión 1.9 y Resolución DIAN 000085 del 8 de abril de 2022, y las normas que modifiquen o sustituyan.

De acuerdo con lo anterior el procedimiento aplicable deberá cumplir con las siguientes características:

- xxi. El valor del bien(es) y/o servicio(s) se cobrará iniciando con la suscripción por las partes del Acta de Recibo a Satisfacción de los bienes y/o servicios contratados, para lo cual **el Contratista** elaborará y remitirá a **ETB** la factura electrónica de venta o documento equivalente electrónico correspondiente, aprobada previamente por el Supervisor de **ETB**.

La factura electrónica de venta o documento equivalente electrónico deberá reflejar todos los descuentos a que haya lugar de forma que la misma sea coincidente en toda su información con el Acta incluida en el proceso de radicación.

- xxii. En línea con lo señalado por las normas vigentes; y sujeto a los cambios que se presenten durante la ejecución del contrato, de forma que cualquier modificación de ley promulgada con posterioridad a su formalización le será aplicable; **el Contratista** deberá proceder para la radicación de su facturación en los términos detallados a continuación:

La factura electrónica de venta o documento equivalente electrónico y el Acta de recibo a satisfacción serán radicadas en el portal web que el Equipo Cuentas por Pagar de ETB destine para ello, la fecha máxima de radicación mensual es determinada en el cronograma de cierre contable mensual que define la Empresa y que será comunicado desde la Supervisión del Contrato, de acuerdo con lo anterior para dar continuidad al proceso es necesario integrar la totalidad de los documentos relacionados continuación y que corresponden a:

- El formato XML AttachedDocument de su factura electrónica de venta o documento equivalente electrónico con el documento validado por la DIAN.
- La representación gráfica de la factura electrónica de venta o documento equivalente electrónico (Archivo PDF)
- El Acta de pagos formalizada por las partes.
- El número(s) de pedido(s) y hoja(s) de entrada.
- Otros documentos que apliquen de acuerdo con los términos acordados por las partes en el presente contrato y sus anexos y/o documentos complementarios.
- Los contratistas personas naturales que presten servicios, deberán adjuntar la certificación de que trata el Decreto 1625 de 2016 y el Decreto 2231 de 2023. A

partir de esta certificación se determinará la retención en la fuente a título de renta a aplicar sobre el pago o abono en cuenta.

**xxiii.** Así mismo y atendiendo lo señalado por las mencionadas Resoluciones y específicamente en el “Anexo Técnico de Factura Electrónica de Venta versión 1.9”, ETB ha dispuesto el correo electrónico [recepcionfacturas@etb.com.co](mailto:recepcionfacturas@etb.com.co) destinado como buzón automático único para este proceso y en el cual no se atenderán asuntos diferentes al procesamiento de documentos a radicar, es indispensable señalar que si se ha realizado radicación por medio del Portal WEB ya indicado en el literal (B), no se debe tramitar la misma solicitud por el correo electrónico dado que las dos opciones son excluyentes entre sí. La radicación por cualquiera de los dos medios se realizará únicamente en días hábiles y en las fechas que defina la administración.

Es necesario que, para el procedimiento de radicación por medio de correo electrónico, el proveedor se asegure de incluir en un único archivo .ZIP la siguiente información:

- El formato XML AttachedDocument de su factura electrónica de venta o documento equivalente electrónico con el documento validado por la DIAN. En el mismo debe diligenciarse:
  - j) En el campo “cbc: ElectronicMail” del formato XML AttachedDocument incluya su dirección de correo para respuestas de aceptación o rechazo. *Importante:* Sí esta información no es señalada o corresponde a un correo electrónico de tipo automático, ETB no podrá comunicar el estado de su trámite.
  - k) En el campo “Order Reference” del archivo XML integre el número de pedido, de referirse a más de un pedido incluya cada uno separado por punto y coma (;).
  - l) En el campo “Receipt Document” Reference” del archivo XML integre el número de entrada, de referirse a más de una entrada incluya cada una de las mismas separadas por punto y coma (;).
- En otro archivo .ZIP al interior del indicado en el literal (i)
  - La representación gráfica de la factura electrónica de venta o documento equivalente electrónico (Archivo PDF)
  - El Acta de pagos formalizada por las partes.
  - Otros documentos que apliquen de acuerdo con los términos acordados por las partes en el presente contrato y sus anexos y/o documentos complementarios.

Para su información el proceso de validación de ETB, tanto mediante portal WEB como mediante correo electrónico, verificará:

- i) La existencia de un único archivo .ZIP al interior del correo electrónico con el XML AttachedDocument de su factura electrónica de venta o documento equivalente electrónico, validado por la DIAN.
- j) La existencia de un archivo .ZIP al interior del .ZIP previamente mencionado con la representación gráfica de la factura (Archivo PDF) y su coincidencia exacta con el XML AttachedDocument.

Canales de radicación oficial:

Físico: Carrera 8 No 20 - 56 Piso 1 Ventanilla de Correspondencia

Digital: [gestioncorrespondencia@etb.com.co](mailto:gestioncorrespondencia@etb.com.co)



- k) La inclusión del Acta de pagos (Archivo PDF) formalizada y su coincidencia exacta con los dos ítems anteriores.
- l) La validez y exactitud de la información relacionada con pedido(s) y hoja(s) de entrada.

Si alguna de estas condiciones no se cumple la factura electrónica de venta o documento equivalente electrónico no podrá ser radicada y por ende no se podrá dar continuidad al proceso de radicación, en este caso el proveedor recibirá, a la dirección de correo reportada en el AttachedDocument, el rechazo de su trámite.

Es responsabilidad del proveedor informar, en el campo "cbc: ElectronicMail" del formato XML AttachedDocument una dirección electrónica que corresponda a un buzón activo y no de respuesta automática, si la información del correo electrónico no es integrada o no cumple las condiciones señaladas ETB no podrá asegurar el seguimiento que el proveedor pueda realizar al proceso.

ETB tendrá la posibilidad de presentar objeciones o rechazos a las facturas radicadas en los términos de generación de eventos definidos por la DIAN en relación con la facturación electrónica, procedimiento que se realizara mediante contacto a la dirección electrónica informada por **el Contratista** al momento de radicar en la plataforma de ETB o como parte de la información remitida al correo electrónico, en los términos previamente mencionados en el literal (C), el proveedor procederá a realizar las correcciones respectivas y presentará una nueva factura electrónica dentro de los plazos para radicación establecidos por el área de cuentas por pagar de ETB la cual se pagará de acuerdo con el plazo señalado en el contrato y/o en los términos de referencia, y una vez atendida a la radicación y aceptación en los términos previamente descritos.

07-07.7-F-025-v.7

01/08/2025

"Una vez impreso este documento, se considerará **documento no controlado**".

## CAPÍTULO III - CONDICIONES TÉCNICAS

### 3.1 PRESENTACIÓN DE OFERTA EN LA ETAPA DE TÉRMINOS DEFINITIVOS

El oferente tiene la responsabilidad de revisar, analizar, interpretar y entender en su totalidad las especificaciones y condiciones establecidas en los Términos de Referencia y en los documentos anexos que los conforman. Esto con el fin de presentar una oferta que sea completa, económicamente sostenible, integral y ejecutable, acorde con las obligaciones exigidas en dichos documentos.

La Oferta deberá ser presentada en castellano; no obstante, podrán anexarse catálogos en inglés.

El OFERENTE debe tener en cuenta que las respuestas que suministre en este capítulo deben corresponder con el equipamiento y licenciamiento para la implementación de proyectos, constituyéndose en parte de su oferta y por lo tanto del contrato que pueda celebrarse.

**3.2 REQUISITOS HABILITANTES:** el oferente debe presentar junto con la oferta los requisitos exigidos para acreditar el cumplimiento en los grupos en los cuales se presente.

**3.3 REQUISITOS OBLIGATORIOS DE EJECUCIÓN, SEGUIMIENTO Y CONTROL:** el oferente debe aceptar con la presentación de la oferta en los grupos que aplique los requisitos de ejecución sin condicionamiento alguno, por tanto, en la ejecución del contrato se obliga a cumplirlos de conformidad con las estipulaciones de los términos de referencia, adendas y anexos.

### 3.4 EVALUACIÓN TÉCNICA DE OFERTA

ETB llevará a cabo la evaluación de las ofertas técnicas con base en la verificación del cumplimiento **de los requisitos habilitantes del Oferente** y de los requisitos **obligatorios relacionados con la ejecución, seguimiento y control**, conforme a lo establecido en los presentes Términos de Referencia.

ETB tendrá en cuenta la completitud en el cumplimiento de los requerimientos solicitados en el presente documento, así como la documentación de respaldo correspondiente, incluidas las cartas de los fabricantes y los certificados de experiencia.

Durante la etapa de evaluación, ETB podrá solicitar al oferente, a través de mensajes en el evento correspondiente en la herramienta SAP Ariba, las aclaraciones, explicaciones o cursar los requerimientos que considere necesaria.

El oferente deberá atender las solicitudes de ETB dentro del plazo estipulado, utilizando exclusivamente los mensajes del evento creado en SAP Ariba. En caso de que, a partir de la respuesta, se concluya que el requerimiento no fue completamente satisfecho o que su cumplimiento está sujeto a alguna condición, la oferta será rechazada.

Canales de radicación oficial:

Físico: Carrera 8 No 20 - 56 Piso 1 Ventanilla de Correspondencia

Digital: [gestioncorrespondencia@etb.com.co](mailto:gestioncorrespondencia@etb.com.co)



ETB se reserva el derecho de solicitar al oferente una presentación con el fin de aclarar los aspectos técnicos de la propuesta; no obstante, dicha presentación no podrá implicar modificaciones a la oferta presentada.

El resultado de la evaluación será “CUMPLE” o “NO CUMPLE”, con base en la verificación del cumplimiento de los requisitos habilitantes y obligatorios relacionados con la ejecución, seguimiento y control.

### 3.5 ANTECEDENTES

El sector de la conectividad y los servicios digitales enfrenta una disrupción sistémica. El modelo tradicional, centrado en la conectividad, enfrenta una comoditización acelerada y márgenes decrecientes. La evolución hacia una Techco un integrador de verticales de transformación digital de alto valor que usa la conectividad como plataforma ha dejado de ser una opción estratégica para convertirse en un imperativo de supervivencia y liderazgo.

Este proceso de contratación es la piedra angular de dicha transformación. Su objetivo es dotar a ETB de las capacidades para competir no en el precio del ancho de banda, sino en el valor de las soluciones integrales ofrecidas por ETB .

Este modelo de alianza, por tanto, trasciende la relación transaccional para forjar asociaciones estratégicas de largo plazo. El objetivo es seleccionar un ecosistema de aliados best-in-class; no buscamos intermediarios, sino líderes que demuestren superioridad técnica y propiedad intelectual (productos propios). Se priorizará socios con portafolios de múltiples servicios integrables, capaces de construir soluciones end-to-end.

El acuerdo marco se enfocará en alianzas que generen sinergias operativas tangibles. La habilitación de economías de escala es un factor crítico que debe impactar directamente en la optimización de la rentabilidad y la expansión de márgenes en estos nuevos verticales de negocio.

Un pilar de esta asociación es la generación de demanda conjunta. Buscamos socios que demuestren un compromiso proactivo con la expansión de la generación de oportunidades. No es una relación pasiva; es una colaboración comercial donde los activos de ETB nuestra experiencia probada, el posicionamiento de marca y el acceso estratégico a contratos interadministrativos sirvan como plataforma de lanzamiento.

ETB se posiciona como el socio catalizador para la expansión conjunta.

Para materializar esta captura de mercado, el modelo priorizará socios que demuestren su compromiso a través de fondos de marketing (MDF). Esto se estructurará como una co-inversión destinada a financiar estrategias de go-to-market (GTM), acelerar la generación de demanda y maximizar la penetración de las soluciones.

Finalmente, la sostenibilidad de esta transformación se fundamenta en una transferencia efectiva de conocimiento. Un socio estratégico invierte en la autonomía de su contraparte. El modelo exigirá un proceso riguroso de alta capacitación y mentoría. El objetivo es que ETB, a través de su PMO y equipos técnicos, logre la apropiación metodológica y

07-07.7-F-025-v.7

01/08/2025

*“Una vez impreso este documento, se considerará **documento no controlado**”.*

operativa del core de las soluciones. Esto es indispensable para reducir la dependencia y garantizar nuestra soberanía tecnológica a largo plazo.

Este modelo nos dará la agilidad para reducir los ciclos de contratación de semanas a días, un factor decisivo para competir con la velocidad que el mercado digital exige.

### 3.6 OBJETIVO

En el marco de su estrategia de **transformación digital**, ETB está fortaleciendo su rol como socio tecnológico de sus clientes. Para ello, busca expandir y modernizar su portafolio de servicios gestionados, con un enfoque en la integración de soluciones de vanguardia.

El ACUERDO MARCO con aliados estratégicos, está orientado a la provisión de servicios que soporten las siguientes áreas clave:

- Grupo I: Infraestructura y Software en modalidad de Servicio
- **Grupo II: Ciberseguridad**
- Grupo III: Nubes Privadas
- Grupo IV: Gestión de Procesos de Negocio (BPO)
- Grupo V: Desarrollo de Software a la medida
- Grupo VI: Ciudad 360
- Grupo VII: Servicios especializados
- Grupo VIII: Smartphones como servicio
- Grupo IX: Servicios de Conectividad Avanzada (SDWAN as a service)
- Grupo X: Smart Citys
- Grupo XI: Gobierno y Empresa Inteligente
- Grupo XII: E-HEALTH
- Grupo XIII: ED TECH
- Grupo XIV: Últimas Millas Conectividad.

Para lograr este objetivo, ETB mediante la presente invitación pública convoca a la presentación de ofertas a aliados estratégicos que puedan proveer, bajo un modelo de prestación de servicios, arrendamiento o suscripción, la infraestructura y las plataformas tecnológicas necesarias. Los componentes técnicos y tecnológicos de las soluciones ofertadas deben cumplir con los siguientes requisitos:

- **Tecnología de vanguardia:** Los equipos, plataformas y servicios deben ser de última generación, incorporando capacidades de Inteligencia Artificial (IA) y Aprendizaje Automático (Machine Learning) para optimizar el rendimiento, la seguridad y la gestión operativa.
- **Garantía y Soporte:** Se requiere que todos los componentes técnicos/tecnológicos cuenten con el soporte y la garantía directa del fabricante durante toda la vigencia del contrato.
- **Licenciamiento y Componentes Mínimos:** La solución debe incluir todos los licenciamientos y componentes de hardware y/o softwares necesarios para su correcta y completa operación.

- **Gestión y Monitoreo:** Las plataformas, equipos y servicios deben proveer herramientas de gestión y monitoreo centralizadas que permitan una administración eficiente, la generación de informes y la supervisión proactiva.

Este enfoque permite a ETB integrar soluciones escalables, confiables y tecnológicamente avanzadas, garantizando la continuidad y manteniendo la excelencia en la prestación del servicio que caracteriza a la Compañía.

Lo anterior con el propósito de generar economías de escala, optimizar recursos y aprovechar sinergias que fortalezcan la eficiencia operativa y la capacidad de negociación en beneficio del conjunto empresarial, con fundamento en un modelo de gobierno con las filiales y con las Empresas en que ETB tenga participación es de una operación involucrada, es decir, operar los negocios de forma integrada desde el núcleo corporativo teniendo en cuenta la unidad de propósito y habilitación de palancas y criterios de beneficio mutuo.

En consecuencia, y para efectos de facilitar el relacionamiento de las distintas personas jurídicas que integran el Grupo Empresarial o sobre las que ETB ostenta participación, conviene a todos sus integrantes contar con un mecanismo de agregación de demanda y ventajas competitivas.

Las condiciones establecidas en el Acuerdo Marco de Precios podrán ser utilizadas no solo por ETB, sino también por sus filiales, subordinadas, empresas del Grupo Empresarial ETB y aquellas en las que ETB tenga participación accionaria. Esto para los grupos en los que estas empresas no hayan sido adjudicatarias.

Cada empresa participará según su interés en la ejecución de los Acuerdos Marco haciendo uso de la expedición de órdenes de servicio según necesidades con la finalidad de obtener las ventajas propias del Mecanismo de agregación de demanda, como las economías de escala, conocimiento, experiencia, aspectos de tecnología, destreza, entre otros aspectos.

Las transacciones celebradas para el uso de los Acuerdos Marco se denominan “Órdenes de Servicio”, que se derivan de la ejecución de las diferentes líneas de negocio referidas en el numeral 2 del presente documento, negocios jurídicos enmarcados en criterios de racionalidad económica.

En cada orden se establecerán los términos y condiciones de las particularidades y alcance del servicio solicitado, definiéndose en ella valor, forma de pago, plazo, cronogramas, metodologías, recursos que se requieren, acuerdos de niveles de servicio y las demás condiciones propias de los servicios requeridos.

### 3.7 GRUPO II: CIBERSEGURIDAD

Un servicio integral de ciberseguridad es fundamental para proteger los activos digitales de una organización. A continuación, se detallan los componentes mínimos,

funcionalidades, y especificaciones técnicas necesarias para garantizar la seguridad, disponibilidad y resiliencia de la infraestructura de TI.

### 3.7.1 REQUISITOS MÍNIMOS HABILITANTES DEL OFERENTE

El OFERENTE debe responder describiendo de qué forma se cumplirán los requerimientos adjuntando catálogos, fichas técnicas y demás documentación que soporte la respuesta.

1. Se requiere que el interesado haga llegar con su oferta las certificaciones de distribuidor o partner de los fabricantes que sustentan su oferta de servicios.
2. Se requiere que el interesado haga llegar con su oferta su certificación ISO 27000:2022.

### 3. EXPERIENCIA MÍNIMA HABILITANTE DEL OFERENTE

EL OFERENTE debe acreditar experiencia mediante certificaciones de contratos cuyo objeto guarde relación directa con la prestación del servicio de ciberseguridad, que hayan sido suscritos dentro de los dos (2) años anteriores a la fecha de presentación de oferta. Para tal efecto, se aceptan mínimo una y máximo cinco (5) certificaciones que sumen \$4.000.000.000 pesos (antes de IVA).

#### REQUISITOS DE LAS CERTIFICACIONES

- Deben ser expedidas a nombre del OFERENTE por la empresa o entidad a las que se les haya prestado el servicio, y ser firmadas por el responsable de la entidad contratante
- Expedidas y firmadas, a quien el OFERENTE suministre los bienes o servicios. "Una vez impreso este documento, se considerará documento no controlado".
- Debe contener: el objeto asociado a cada una de las líneas de negocio, el año de celebración o ejecución del contrato y el valor.

Nota 1: cuando EL OFERENTE presente documentos de contratos en los cuales prestó servicios o suministró bienes en cualquier modalidad de asociación, consorcio o unión temporal entre otros, el requisito de experiencia a evaluar corresponderá únicamente al porcentaje en que haya participado EL OFERENTE. En tal sentido en la respectiva certificación que aporte deberá reflejarse el porcentaje de participación que tuvo en la asociación.

Nota 2: en caso de que la experiencia se origine de contratos celebrados entre EL OFERENTE y ETB, se debe relacionar cada uno de los requisitos solicitados e informar el o los números de contratos con el fin de verificar el requisito de experiencia solicitado al interior de ETB.

Nota 3: las certificaciones expedidas en el exterior deben ser emitidas en el idioma del país de origen, apostilladas o legalizadas y traducidas oficialmente al castellano.

Nota 4: para las certificaciones emitidas en moneda extranjera, ETB realizará la conversión a pesos colombianos utilizando la Tasa Representativa del Mercado publicada por el Banco de la República de Colombia, en la fecha de suscripción del contrato o de la prestación de servicios conforme a las fechas que obren en cada certificación. Nota 5: ETB se reserva el derecho de verificar la información suministrada por EL OFERENTE y de solicitar las aclaraciones que considere

conveniente. En caso de que la información no sea veraz, la oferta será rechazada. Nota 6: no se tendrán en cuenta experiencias anónimas, así el CONTRATISTA alegue razones de confidencialidad. Nota 7: No se tendrán en cuenta auto certificaciones.

### 3.7.2 REQUISITOS OBLIGATORIOS DE EJECUCIÓN SEGUIMIENTO Y CONTROL

#### 3.7.2.1 Soporte preventa de los servicios o soluciones que forman parte del acuerdo marco

El Aliado especializado en Infraestructura y Software en modalidad de servicio debe ofrecer distintos mecanismos que soporten el diseño de soluciones, así como la realización de demostraciones que garanticen la comprensión y beneficios operativos alineados con las necesidades técnicas, operativas y estratégicas de ETB. Estas actividades deben contribuir a la concreción de soluciones robustas, estables y alineadas con las necesidades de ETB y de sus clientes en los casos en los que ETB integra soluciones tecnológicas. Así pues, el soporte a la preventa aumenta la probabilidad de que la solución ofrecida por el Aliado incremente la posibilidad de que la oferta resulte técnicamente viable y competitiva, lo que hace que posicione al contratista como un Aliado Estratégico y no como un proveedor. Sin perjuicio de las actividades que adicionalmente puede desarrollar el Aliado, las actividades que contribuyen a los objetivos propuestos son las siguientes:

- Diseño de las soluciones precisas, estables, minimizando riesgos, identificando integraciones necesarias y elementos requeridos para una correcta implementación y funcionamiento.
- Presentación de Demos o de pruebas de concepto, lo cual pretende validar la efectividad de la solución, lo que permite confianza y seguridad para la adquisición con el Aliado Estratégico. Adicionalmente, esto fortalece el relacionamiento de toda la cadena de abastecimiento hasta la satisfacción de las necesidades.
- Impulsar el performance de ETB mediante el fortalecimiento y la ejecución de estrategias de marketing conjunto con el Aliado Estratégico.
- Soporte técnico al equipo preventa de ETB
- Entrenamiento del distribuidor o del fabricante en productos de línea base que forman parte del ACUERDO MARCO coordinadas previamente con el equipo ETB.
- El ALIADO deberá transferir el conocimiento al equipo ETB para el diseño, arquitectura y manejo de herramientas preventa que apoyen el desarrollo de las ofertas en conjunto y el desarrollo del conocimiento del equipo ETB.
- Dimensionamiento técnico de infraestructura y/o servicios de acuerdo con la necesidad del cliente final ETB, actividad realizada en conjunto con el equipo preventa ETB.
- Diseño de soluciones tecnológicas que cumplan con la expectativa de cliente final.
- Actualización de alcance técnico de productos ofertados al equipo preventa ETB
- Preparación de Quotes de fabricantes
- Suministro de documentación técnica de productos y/o servicios ofertados
- Escalamiento y solución con fabricantes en los casos que se requiera
- Elaboración de de una propuesta técnica detallada de la tecnología que sea compatible con las integraciones que ETB realiza.
- Suministro de cronograma general de entrega de las soluciones.

- El oferente deberá apalancar las iniciativas comerciales de ETB para la generación de demanda y cierre de negocios a través de la participación de los eventos que se mapeen en conjunto y de los fondos de mercadeo provistos por los fabricantes para dicho fin.
- El oferente deberá proveer al equipo ETB laboratorios técnicos, salas para workshops y equipos DEMO con los cuales el equipo de ETB designado pueda hacer pruebas de concepto para los clientes ETB y afinar las características de los productos que se ofertan con cada uno de los fabricantes habilitados.
- El oferente deberá proveer salas de reuniones en sus instalaciones, o locaciones adecuadas para realizar actividades comerciales con clientes ETB, en los cuales ETB pueda desarrollar una agenda conjunta con el oferente y el o los fabricantes habilitados.
- El oferente deberá destinar el equipo necesario para que acompañe los requerimientos técnicos asociados al alcance de este contrato.

### 3.7.2.2 PROCEDIMIENTO PARA ORDENES DE SERVICIO

ETB podrá solicitar a los Aliados Estratégicos con ACUERDO MARCO suscrito la presentación oferta bajo las mismas condiciones. Dicha oferta deberá presentarse dentro de los 3 días siguientes a la solicitud o, por medio de la herramienta tecnológica indicada, y deberá contener los respectivos descuentos con base en los precios unitarios pactados en el acuerdo marco. La presentación de ofertas es obligatoria por parte del Aliado Estratégico.

Dentro de los dos (2) días hábiles siguientes al recibo de la Oferta, ETB verificará el cumplimiento de todos los requisitos y, de ser necesario, adelantará la negociación dentro de los dos (2) días hábiles siguientes, garantizando la igualdad de condiciones entre los Aliados de cada grupo. Posteriormente, la orden de servicio será asignada al Aliado que ofrezca las mejores condiciones económicas.

Si se presenta un empate entre dos o más ofertas al efectuar la sumatoria de la ponderación establecida según corresponda, ETB utilizará las reglas de forma sucesiva y excluyente para seleccionar el oferente, de conformidad con lo establecido en el artículo 35 de la Ley 2069 de 2020 reglamentado por el artículo 2.2.1.2.4.2.17 del Decreto 1860 de 2021.

Por lo anterior, el ALIADO deberá presentar junto con la oferta la documentación con la que pretenda acreditar alguno de los criterios de desempate, con el fin de que, en caso de presentarse empate la misma sea revisada de conformidad con las reglas de la citada norma.

Si persiste el empate, como mecanismo aleatorio de desempate, se utilizarán las siguientes reglas:

- ETB dispondrá de balotas debidamente numeradas.
- La numeración de las balotas iniciará en el número 1 y continuará en orden ascendente.
- El delegado de ETB, en presencia de todos los oferentes que se encuentren empatados en puntos, introducirá las balotas numeradas en una bolsa de color negro.
- El número de balotas introducidas será el doble del número de oferentes empatados en puntos.
- Al momento de la diligencia, los oferentes deberán acreditar la facultad legal para participar.

- La participación para tomar la balota de la bolsa se hará en orden alfabético, teniendo en cuenta la primera letra del primer apellido o de la razón social del oferente, sea éste persona natural, jurídica, consorcio o unión temporal.
- Una vez el oferente tome la balota de la bolsa la tendrá en su poder sin hacer público el número sacado, hasta tanto no hayan tomado la balota todos los participantes.
- Posterior a esto, se hará pública la numeración de las balotas que los oferentes tienen en su poder.
- El empate se resolverá a favor del oferente que haya sacado la balota marcada con el mayor número.
- De todo lo actuado se levantará la respectiva acta, con la firma de todos los participantes.

Finalizada la revisión técnica (cuando aplique) y financiera, se remitirá a los aliados el resultado, indicando si se le asigna o no la orden de pedido y/o servicio.

ETB se reserva el derecho de solicitar cotización a un solo Aliado en aquellos casos en los que se requiera garantizar la continuidad en la prestación del servicio o cuando sea necesaria la integración de soluciones. En tales eventos, ETB deberá justificar internamente las razones objetivas que sustenten dicha decisión dentro del marco legal vigente aplicable a ETB.

De forma previa a la formulación de orden de servicio ETB incorporará los recursos al contrato y será requisito para la ejecución la constitución de las garantías correspondientes.

**Parágrafo Primero:** La solicitud de cotización constituye una invitación a los Aliados a presentar oferta en las condiciones requeridas, incluyendo el descuento respectivo. En este sentido, ETB no adquiere compromiso alguno de continuar con el procedimiento, ni de concluirlo mediante la emisión de una orden de servicio o pedido. ETB podrá dar por terminado el procedimiento en cualquier momento, sin aceptar oferta alguna y sin que haya lugar a reconocimiento económico para los Aliados, quienes aceptan esta estipulación con la presentación de su oferta.

ETB podrá suspender o terminar, por decisión interna, la solicitud de cotización u orden de compra cuando aparezcan circunstancias que hagan inconveniente la contratación, tales como: razones técnicas, operativas, económicas, de mercado, fuerza mayor, orden de autoridad competente, acto irresistible de terceros o razones de utilidad o conveniencia corporativa.

**Parágrafo Segundo:** Tratándose de órdenes de servicio derivadas de los acuerdos marco para necesidades de empresas que hagan parte del conjunto empresarial y/o en aquellas en las que ETB tenga participación, la Solicitud (que detalle la necesidad, conveniencia, valor estimado y plazo, entre otros aspectos) y la línea de negocio identificada, deben remitirse a la Dirección de Abastecimiento o quien haga sus veces, con una antelación no menor a diez (10) días a la necesidad de la expedición de dicha orden.

### 3.8 MODELO DE GESTIÓN DE CIBERSEGURIDAD

Dentro del modelo de gestión de ciberseguridad, se contempla una arquitectura basada en capas, cubriendo la prevención, detección, respuesta y recuperación. Cada componente es fundamental para asegurar la disponibilidad, confidencialidad e integridad del servicio.

Los servicios objeto de cotización son integrales, lo que implica que el interesado deberá dimensionar los costos contemplando todos los recursos lógicos, físicos, profesionales y demás que demande el servicio, necesarios para la ejecución de las actividades, teniendo en cuenta que, el alcance comprende la prestación de servicios acorde con las actividades técnicas descritas y que en todo caso, el Proveedor es el responsable frente a las garantías que como empleador le asiste con respecto a sus trabajadores con quienes preste el servicio. En todo caso, el valor máximo a pagar por los servicios frente a un eventual contrato será el cotizado por el interesado.

Los servicios ofrecidos por el Proveedor deben permitir la **interoperabilidad** con los sistemas existentes de la organización y con las soluciones de seguridad de otros proveedores líderes en el mercado.

Los servicios de seguridad desplegados deberán ser **portables** en la medida de lo posible, permitiendo:

- b) La migración de configuraciones y políticas de seguridad.
- c) La portabilidad de los agentes de protección instalados en los diferentes activos.
- d) La transferencia de la configuración de red y las reglas de acceso.
- e) La portabilidad de los componentes de software de seguridad instalados sobre la plataforma, excluyendo los recursos subyacentes como hipervisores y hardware.

Esto asegura que la protección pueda ser replicada o migrada entre diferentes entornos (nube, local, híbrido) sin la necesidad de una reconfiguración total, optimizando la flexibilidad y la capacidad de respuesta ante cambios en la infraestructura.

### 3.8.1 EQUIPOS DE CIBERSEGURIDAD

ETB busca contar con una oferta de equipos y tecnologías que soporten y fortalezcan la oferta de valor de ciberseguridad para nuestros clientes externos e internos, a continuación, se detallan los elementos que de acuerdo con el conocimiento del mercado cuentan con mayor rotación.

- ☐ **FIREWALL:** es un sistema de seguridad que funciona como un "puerta de acceso" para las redes, controlando el tráfico de datos entrante y saliente basándose en reglas predefinidas para proteger una red confiable (como la de tu casa u oficina) de una red no confiable (como Internet). Puede ser un dispositivo físico (hardware) o un programa (software) y su propósito principal es filtrar y bloquear accesos no autorizados, actividades maliciosas y amenazas cibernéticas, actuando como una barrera para mantener segura la información. El equipo puede ser instalado para entornos de TI o para entornos externos.

#### ✓ **Funcionalidades Mínimas**

- Firewall de Próxima Generación (NGFW): Inspección de paquetes profunda (DPI) en las capas de red y aplicación.

- Sistema de Prevención de Intrusiones (IPS): Detección y bloqueo automático de amenazas conocidas y vulnerabilidades.
  - Antimalware y Antivirus: Protección en tiempo real contra software malicioso, incluyendo virus, ransomware y troyanos.
  - Filtrado de Contenido Web y URL: Bloqueo de sitios web maliciosos o inapropiados para la política de la empresa.
  - Control de Aplicaciones: Capacidad para identificar y controlar el uso de aplicaciones en la red, independientemente del puerto o protocolo.
  - VPN (Red Privada Virtual): Creación de túneles seguros y encriptados para el acceso remoto a la red corporativa.
  - Análisis de Amenazas (Threat Intelligence): Uso de bases de datos de amenazas actualizadas en tiempo real para la detección proactiva.
  - Sandboxing: Aislamiento de archivos sospechosos en un entorno seguro para su análisis antes de que ingresen a la red.
  - Seguridad en la Nube: Integración con entornos de nube pública y privada.
- ✓ **Elementos mínimos de la gestión del servicio**  
El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:
- Hardware/Software de última generación.
  - Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
  - Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
  - Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.
- ✓ **Alcances Técnicos**
- Alta Disponibilidad (HA): De acuerdo con el requerimiento de ETB o su cliente, el servicio de FW debe ser redundante, con un sistema de failover (conmutación por error) automático para garantizar la continuidad del servicio.
  - Capacidad de Conexión y Rendimiento: El equipo debe ser capaz de manejar el tráfico de la red sin degradación del rendimiento.
  - Enrutamiento (Routing): Debe soportar protocolos de enrutamiento dinámico como OSPF y BGP.
  - VPN: Se debe soportar túneles VPN tipo IPSec y SSL-VPN para la conectividad sitio a sitio y de usuarios remotos.
  - Inspección SSL: El Firewall debe ser capaz de inspeccionar el tráfico encriptado con SSL/TLS para detectar amenazas ocultas.
- ✓ **Fabricantes y Plataformas**  
El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos ejemplos de fabricantes con plataformas que cumplen estos requisitos son:
- Palo Alto Networks: con su plataforma Strata (NGFW).
  - Fortinet: con su plataforma FortiGate.
  - Cisco: con la línea de Firewalls ASA y Firepower.
  - Check Point: con su familia de productos Quantum.
  - Juniper Networks: con la serie SRX.
  - Hillstone

- Sophos
- SonicWall

### ✓ **Funcionamiento y Configuraciones**

- Políticas de Seguridad: El proveedor deberá colaborar en la creación e implementación de políticas de seguridad basadas en las necesidades del cliente.
- Administración Centralizada: Se deben utilizar herramientas que permitan la administración centralizada de todos los equipos y las políticas de seguridad.
- Reportes y Auditoría: El servicio debe generar reportes periódicos sobre la actividad de la red, los intentos de intrusión y el cumplimiento de las políticas.
- Arquitectura de Implementación: El Firewall debe poder ser implementado en modo inline (en línea) para la inspección de todo el tráfico de entrada y salida, o en modo tap (toma de tráfico) para monitoreo pasivo.

☐ **EPP - EDR:** Se busca una solución que combine las capacidades de una Plataforma de Protección de Endpoints (EPP) y una de Detección y Respuesta en Endpoints (EDR) para una defensa profunda. El objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de los activos de la información.

### ✓ **Requerimientos Técnicos y Funcionales Mínimos**

- **Funcionalidades de la Plataforma de Protección de Endpoints (EPP)**
  - Motor Antivirus/Antimalware: Protección en tiempo real contra virus, gusanos, troyanos y ransomware. Debe utilizar múltiples técnicas de detección, incluyendo firmas, heurística, y análisis de comportamiento.
  - Firewall Personal: Controlar el tráfico de red en los endpoints para prevenir accesos no autorizados.
  - Control de Dispositivos: Gestionar el uso de dispositivos de almacenamiento extraíbles (USB, discos duros externos) para prevenir la fuga de datos o la entrada de malware.
  - Análisis de Vulnerabilidades: Identificar y reportar las vulnerabilidades del software y las configuraciones de seguridad en los endpoints.
- **Funcionalidades de Detección y Respuesta en Endpoints (EDR)**
  - Monitoreo Continuo: Recopilar datos de actividad de los endpoints en tiempo real, incluyendo procesos en ejecución, conexiones de red, cambios en el registro y en los archivos.
  - Detección de Amenazas: Utilizar Inteligencia Artificial (IA) y Aprendizaje Automático (Machine Learning) para identificar comportamientos sospechosos o anómalos que puedan indicar una amenaza avanzada (como ataques sin archivos o movimientos laterales).
  - Análisis Forense: Proporcionar capacidades de análisis forense para investigar el origen, la trayectoria y el impacto de un ataque. Esto incluye la capacidad de buscar amenazas históricas en los datos recopilados (Threat Hunting).

- o Respuesta Automatizada: Ejecutar acciones de respuesta inmediatas, como aislar un dispositivo infectado de la red, finalizar un proceso malicioso o eliminar un archivo.
  - o Remediación: Permitir la limpieza y restauración de los endpoints a un estado seguro después de una infección.
- **Consola de Gestión Centralizada**
    - o Gestión Unificada: Una única consola que permita la administración de la EPP y EDR.
    - o Informes y Alertas: Generación de informes detallados sobre incidentes de seguridad, estado de los endpoints y cumplimiento de políticas. Se requieren alertas en tiempo real para los equipos de seguridad.
    - o Escalabilidad y Flexibilidad: La solución debe ser escalable para soportar un número creciente de endpoints y poder desplegarse en diferentes sistemas operativos (Windows, macOS, Linux, Android, iOS).
- ✓ **Pre-requisitos y Alcances Técnicos**
- Infraestructura Requerida: La solución debe ser compatible con la infraestructura de red de la compañía o entidad que solicite el servicio. Se deberán tener en cuenta soluciones SaaS (Software como Servicio) para minimizar la necesidad de infraestructura local.
  - Agente Ligerero (Agent): El software que se instala en los endpoints debe ser ligero, con un consumo mínimo de recursos de CPU y memoria, para no afectar el rendimiento de los usuarios.
  - Integración con SIEM: La plataforma debe contar con APIs que permitan la integración con herramientas de Gestión de Eventos e Información de Seguridad (SIEM) para la correlación de eventos de seguridad.
  - Soporte y Garantía: El proveedor debe garantizar el soporte técnico 24/7 y la actualización continua de la plataforma con las últimas bases de datos de amenazas y funcionalidades.
- ✓ **Funcionamiento y Componentes**
- La solución integral de ciberseguridad funcionará a través de un agente ligero instalado en cada endpoint.
- El agente de EPP previene amenazas conocidas mediante firmas y análisis de comportamiento.
  - El agente de EDR monitorea constantemente la actividad del endpoint y envía los datos a una plataforma centralizada en la nube.
  - En la plataforma centralizada, el motor de análisis de amenazas (impulsado por IA/ML) analiza el comportamiento y detecta anomalías.
  - Al detectar una amenaza, la plataforma genera una alerta y, si está configurada, toma medidas de respuesta automática. El equipo de seguridad puede entonces usar la plataforma para realizar un análisis forense detallado y remediar el incidente.
- ✓ **Elementos mínimos de la gestión del servicio**
- El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:
- Hardware/Software de última generación.

- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

☐ **ANTIDDOS:** es una solución de ciberseguridad que protege a las organizaciones de los ataques de denegación de servicio distribuido (DDoS) mediante la detección y mitigación del tráfico malicioso, antes de que llegue a la red del cliente. Estos servicios, a menudo basados en la nube, actúan como una primera línea de defensa, filtrando el tráfico no deseado y permitiendo el paso del tráfico legítimo para asegurar la continuidad del negocio.

#### ✓ Elementos Mínimos del Servicio

El servicio de Anti-DDoS debe ser provisto como una solución gestionada que incluya los siguientes componentes:

- Sistemas de Detección de Ataques: Plataformas que monitorean el tráfico de red en tiempo real para identificar anomalías y patrones de ataque. Estos sistemas deben ser capaces de detectar ataques de diferentes tipos y volúmenes.
- Mecanismos de Mitigación: Herramientas y dispositivos que se activan para filtrar el tráfico malicioso y permitir que el tráfico legítimo continúe hacia el destino. Esto puede incluir scrubbing centers (centros de limpieza de tráfico) o dispositivos on-premise.
- Portal de Gestión y Monitoreo: Una plataforma que ofrezca visibilidad en tiempo real del estado de la protección, informes de ataques y alertas.
- Soporte y Equipo de Expertos: Un equipo de seguridad 24/7 con experiencia en la mitigación de ataques DDoS, capaz de responder rápidamente a las amenazas.

#### ✓ Funcionalidades de la Solución

- Mitigación por Capas: La solución debe ser capaz de mitigar ataques en las diferentes capas del modelo OSI:
  - Capa 3 y 4 (Volumétricos): Mitigación de ataques que buscan saturar el ancho de banda, como los ataques de inundación UDP, SYN y de reflexión.
  - Capa 7 (Aplicación): Mitigación de ataques que consumen recursos del servidor, como los ataques de inundación HTTP, bots maliciosos y ataques de inyección.
- Detección Automática: El sistema debe detectar los ataques de forma automática y aplicar las contramedidas adecuadas sin intervención manual.
- Adaptabilidad: La solución debe adaptarse a la evolución de las amenazas y ser capaz de mitigar ataques multivectoriales que combinan diferentes técnicas.
- Alta Disponibilidad: El servicio debe garantizar la continuidad de la protección incluso durante fallos del sistema o picos de tráfico.

#### ✓ Fabricantes y Proveedores

El proveedor debe ser un especialista en ciberseguridad, preferiblemente con certificaciones y experiencia probada en la mitigación de ataques a gran escala. Algunos de los principales fabricantes y proveedores en este campo son:

- Cloudflare: Ofrece una red global para la mitigación de ataques en la nube.
- Akamai: Especializado en servicios de protección de aplicaciones web y redes.
- Radware: Proporciona soluciones de mitigación de DDoS tanto en la nube como en hardware.
- Nexusguard: Reconocido por sus soluciones de mitigación a gran escala.

#### ✓ **Funcionamiento del Servicio**

El servicio debe operar de la siguiente manera:

- Monitoreo: El tráfico destinado a la infraestructura de la organización es monitoreado en tiempo real.
- Detección: Cuando se detecta un comportamiento anómalo que coincide con un patrón de ataque, se activa una alarma.
- Redirección de Tráfico: El tráfico sospechoso es redirigido hacia el centro de mitigación del proveedor.
- Mitigación: El tráfico es analizado y "limpiado". El tráfico malicioso es bloqueado, mientras que el tráfico legítimo es enviado de vuelta a la red de la organización.
- Reporte: Se genera un informe detallado del ataque, incluyendo el tipo, la duración, y las acciones de mitigación tomadas.

#### ✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

📄 **ANTISPAM:** Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

#### ✓ **Elementos mínimos requerido de AntiSpam**

Para que el servicio sea completo, debe incluir los siguientes componentes:

- Solución Anti-Spam y Protección de Correo Electrónico: Es el componente principal para filtrar amenazas transmitidas a través del correo electrónico.
- La solución de Anti-Spam debe ser basada en tecnología de propósito específico que facilite la aplicación de funcionalidades de este tipo de servicios.
- Inspección de correo entrante y saliente
- Actualizaciones automáticas de firmas de spam en tiempo real
- Análisis y clasificaciones de reputación de IP

- Autoaprendizaje
  - Definición y modificación de políticas
  - Funcionalidades de antivirus y antispyware
  - Cifrado de correo electrónico
- ✓ **Funcionalidades Clave del Servicio Anti-Spam**  
Una solución anti-spam debe ofrecer las siguientes funcionalidades:
- Filtrado de Spam: Bloquea correos electrónicos no deseados de forma automática.
  - Detección de Phishing: Identifica y bloquea correos electrónicos de phishing que intentan robar credenciales.
  - Análisis de Malware y Virus: Escanea archivos adjuntos y enlaces en busca de código malicioso.
  - Protección contra Ataques de Ingeniería Social (BEC): Detiene ataques que intentan suplantar la identidad de directivos o empleados para realizar transferencias de dinero fraudulentas.
  - Cuarentena de Mensajes: Coloca en una zona segura los correos sospechosos para su revisión antes de ser entregados.
  - Reportes y Estadísticas: Provee informes detallados sobre el volumen de amenazas bloqueadas, los tipos de ataques y la actividad de los usuarios.
- ✓ **Fabricantes y Proveedores**  
El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:
- Microsoft (Microsoft 365 Defender)
  - Fortinet (FortiMail)
  - Cisco (Secure Email)
  - Palo Alto Networks
  - Proofpoint
  - Symantec
- ✓ **Prerrequisitos y Alcances Técnicos**
- Integración: La solución debe integrarse de forma transparente con la infraestructura de correo electrónico existente, ya sea en la nube (ej. Microsoft 365, Google Workspace) o en servidores locales.
  - Escalabilidad: El servicio debe ser escalable para adaptarse al crecimiento de la compañía, tanto en el número de usuarios como en el volumen de correo electrónico.
  - Disponibilidad: La solución debe garantizar una alta disponibilidad, con una redundancia que asegure un funcionamiento continuo y sin interrupciones.
  - Encriptación: Debe ser capaz de cifrar los correos electrónicos sensibles para asegurar que la información no pueda ser interceptada o leída por terceros.
  - Gestión Centralizada: La administración y la configuración del servicio deben poder realizarse desde una plataforma central, lo que simplifica la operación y la supervisión.
- ✓ **Funcionamiento del Servicio Anti-Spam**  
El servicio anti-spam funciona de la siguiente manera:

- Recepción del Correo Electrónico: Cuando un correo electrónico llega al sistema, se redirige al servicio de seguridad antes de llegar a los buzones de los usuarios.
  - Análisis de Amenazas: El servicio analiza el correo en busca de características sospechosas, incluyendo la dirección del remitente, el contenido, los enlaces y los archivos adjuntos.
    - Filtrado: Basado en las políticas de seguridad, el sistema toma una decisión:
    - Permitir: Si el correo es legítimo y seguro, se entrega al buzón del usuario.
    - Cuarentena: Si el correo es sospechoso, se pone en cuarentena para su revisión.
  - Rechazar/Bloquear: Si el correo es claramente malicioso o spam, se rechaza y no se entrega.
  - Entrega Segura: Una vez que el correo ha pasado todas las etapas de filtrado, se entrega de forma segura al usuario.
- ✓ **Elementos mínimos de la gestión del servicio**  
El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:
- Hardware/Software de última generación.
  - Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
  - Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
  - Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.
- 📖 **PROXY:** es un sistema o enrutador que proporciona una puerta de enlace entre los usuarios e Internet. Por lo tanto, ayuda a evitar que los ciber atacantes ingresen a una red privada. Es un servidor denominado “intermediario”, porque está entre los usuarios finales y las páginas web que visitan en línea.
- ✓ **Funcionalidades del Proxy**  
El proxy debe ofrecer un conjunto de funcionalidades críticas para la seguridad y la gestión:
- Filtrado de Contenido: Controlar el acceso a sitios web y aplicaciones basados en categorías (ej. redes sociales, sitios de apuestas).
  - Control de Ancho de Banda: Limitar el consumo de recursos de red por parte de ciertos usuarios o aplicaciones.
  - Registro y Auditoría: Registrar todo el tráfico de la red para análisis de seguridad, cumplimiento y auditoría.
  - Inspección SSL/TLS: Descifrar el tráfico cifrado para inspeccionar su contenido y detectar amenazas ocultas, para luego volver a cifrarlo.
  - Protección contra Malware: Escanear archivos y tráfico en busca de virus, ransomware y otro software malicioso.
- ✓ **Alcances Técnicos y Funcionamiento**  
El servicio de proxy debe ser una solución robusta y escalable que se integre sin problemas con la infraestructura existente.
- Modo de Funcionamiento: El proxy puede operar en modo transparente (sin necesidad de configuración manual en los dispositivos) o explícito (requiere

configuración manual del proxy en cada dispositivo o a través de políticas de red).

- Arquitectura de Alta Disponibilidad: El servicio debe ser redundante para garantizar la continuidad del negocio en caso de fallas de hardware o software. Esto se logra con configuraciones de clúster y balanceo de carga.
- Escalabilidad: La solución debe permitir aumentar la capacidad de procesamiento y almacenamiento para acomodar el crecimiento del tráfico y el número de usuarios.
- Integración con Directorio Activo: Debe sincronizarse con los sistemas de autenticación existentes como Active Directory o LDAP para aplicar políticas de seguridad a nivel de usuario y grupo.

#### ✓ **Fabricantes y Soluciones**

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- Netskope
- Zscaler
- Cloflare
- Skyhigh security
- Fortinet
- Zscaler
- Symantec (Broadcom)
- Cisco

#### ✓ **Requisitos y Componentes Mínimos**

Para que el servicio de ciberseguridad sea completo y funcional, se requieren los siguientes componentes:

- Hardware o Software del Proxy: Los equipos deben ser dimensionados según el número de usuarios y el volumen de tráfico.
- Licenciamiento: Se requieren licencias para las funcionalidades de seguridad, el número de usuarios y el soporte del fabricante.
- Soporte del Fabricante: Se debe contar con un servicio de soporte técnico 24/7.
- Herramientas de Gestión y Monitoreo: La solución debe incluir una consola centralizada para la administración y el monitoreo, con capacidad de generar reportes detallados y alertas en tiempo real.

#### ✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

☐ **WEB APPLICATION FIREWALL:** Un WAF es un firewall de seguridad que protege las aplicaciones web de una variedad de ataques, incluyendo inyecciones de SQL (SQLi), cross-site scripting (XSS), y ataques de denegación de servicio

distribuido (DDoS) a nivel de la capa de aplicación. El WAF actúa como un proxy inverso, inspeccionando el tráfico HTTP/HTTPS entre la aplicación web y el cliente.

#### ✓ **Funcionalidades Mínimas Requeridas**

- Filtrado de Tráfico Malicioso: Capacidad para detectar y bloquear automáticamente ataques comunes basados en el Conjunto de Reglas Principales de OWASP (Open Web Application Security Project).
- Mitigación de DDoS: Funcionalidad para mitigar ataques DDoS en la capa de aplicación (L7), diferenciando el tráfico legítimo del tráfico malicioso.
- Inspección de Contenido (Deep Packet Inspection): Capacidad para analizar el contenido de las solicitudes y respuestas HTTP/HTTPS para identificar patrones de ataque.
- Protección contra Bots: Detección y bloqueo de bots maliciosos que intentan realizar actividades como web scraping, relleno de credenciales o spam.
- Balanceo de Carga: Integración con un balanceador de carga para distribuir el tráfico a múltiples servidores y asegurar la alta disponibilidad de la aplicación.
- Terminación y Cifrado SSL/TLS: El WAF debe ser capaz de gestionar los certificados SSL, descifrar el tráfico para su inspección y volver a cifrarlo antes de enviarlo a los servidores de la aplicación.
- Personalización de Reglas: Permitir la creación de reglas personalizadas para proteger contra amenazas específicas o para adaptarse a la lógica de la aplicación.

#### ✓ **Elementos Mínimos para un Servicio de Ciberseguridad Integral**

- Para que el servicio sea integral, debe ir más allá de un WAF, incluyendo los siguientes componentes de ciberseguridad:
- Gestión de Identidad y Acceso (IAM): Solución que controle el acceso de los usuarios a las aplicaciones y a la infraestructura, con funcionalidades como la autenticación multifactor (MFA) y el acceso con privilegios mínimos.
- Sistema de Detección y Prevención de Intrusiones (IDS/IPS): Software o hardware que monitorea el tráfico de la red para detectar actividades sospechosas o maliciosas y, en el caso del IPS, bloquearlas automáticamente.
- Gestión de Eventos e Información de Seguridad (SIEM): Plataforma que recopila, corelaciona y analiza eventos de seguridad de múltiples fuentes para identificar amenazas, generar alertas y facilitar la investigación de incidentes.
- Análisis de Vulnerabilidades: Servicio periódico de escaneo de vulnerabilidades para identificar debilidades en la infraestructura y las aplicaciones, que deben ser corregidas de manera proactiva.

#### ✓ **Fabricantes y Plataformas**

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- F5 Networks: Conocido por su WAF Big-IP Application Security Manager (ASM) y su plataforma de seguridad de aplicaciones.
- Akamai: Ofrece soluciones de seguridad en la nube que incluyen WAF, protección DDoS y CDN (Content Delivery Network).
- Cloudflare: Plataforma de seguridad y rendimiento en la nube que ofrece servicios de WAF, mitigación de DDoS y protección de bots.

- Imperva: Especializado en la protección de bases de datos y aplicaciones, con un WAF y servicios de seguridad en la nube.
- ✓ **Alcances Técnicos y Requisitos de Servicio**
- Modelo de Despliegue: El servicio puede ser provisto como un servicio gestionado en la nube (SaaS), un dispositivo físico (on-premise) o una solución híbrida. Se valorará la flexibilidad del modelo.
  - Soporte y SLA: Se requiere un Acuerdo de Nivel de Servicio (SLA) que garantice la disponibilidad del servicio (por ejemplo, 99.99%) y un tiempo de respuesta de soporte 24/7 para incidentes críticos.
  - Informes y Analítica: La solución debe proporcionar informes detallados sobre los ataques bloqueados, el tráfico de la red, y el rendimiento del WAF para auditoría y toma de decisiones.
- ✓ **Funcionamiento del Servicio**
- El servicio de ciberseguridad operará bajo un modelo de inspección y control continuo. El tráfico entrante será analizado en tiempo real por el WAF y otros sistemas de seguridad antes de llegar a los servidores de la aplicación. Cualquier actividad sospechosa será bloqueada o alertada. Los logs de seguridad serán centralizados en una plataforma SIEM para su análisis y correlación, permitiendo una respuesta rápida ante incidentes. El monitoreo proactivo garantizará que cualquier nueva amenaza o vulnerabilidad sea abordada de manera oportuna, manteniendo la postura de seguridad de la compañía actualizada.
- ✓ **Elementos mínimos de la gestión del servicio**
- El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:
- Hardware/Software de última generación.
  - Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
  - Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
  - Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.
- ☐ **SANDBOX:** El servicio de Sandbox as a Service (SaaS) debe proveer una plataforma de análisis dinámico de amenazas. Su propósito es ejecutar de manera segura archivos adjuntos, URLs, y otros objetos potencialmente maliciosos en un entorno virtualizado, observando su comportamiento para determinar si son una amenaza real. Esto es crucial para la detección de amenazas de día cero y malware polimórfico que los sistemas de seguridad tradicionales no pueden identificar.
- ✓ **Funcionalidades Clave:**
- Aislamiento y Emulación: El servicio debe crear un entorno virtualizado y completamente aislado (sandbox) que imite un entorno de usuario real, incluyendo sistemas operativos (Windows, Linux, Android) y aplicaciones comunes (navegadores, suites ofimáticas).
  - Análisis Dinámico de Malware: Observa el comportamiento del archivo o URL en tiempo real, registrando acciones como:

- o Cambios en el registro del sistema y en el sistema de archivos.
  - o Conexiones de red salientes y comandos ejecutados.
  - o Intentos de inyección de código.
  - Análisis Estático: Examina el código del archivo sin ejecutarlo para identificar firmas de malware conocidas y anomalías.
  - Generación de Informes: Produce informes detallados con la inteligencia de amenazas, incluyendo el veredicto (benigno, sospechoso, malicioso), el tipo de malware (ransomware, spyware, etc.), y las tácticas, técnicas y procedimientos (TTPs) utilizados, a menudo mapeados al marco MITRE ATT&CK.
- ✓ **Elementos Mínimos del Servicio**
- Para que el servicio de sandbox sea integral, debe contar con los siguientes elementos:
- Motor de Virtualización: La tecnología subyacente que crea los entornos aislados (sandbox).
  - Integración con Otros Controles de Seguridad: Capacidad de integrarse con firewalls de próxima generación (NGFW), sistemas de protección de correo electrónico, gestión de endpoints (EDR) y SIEM/SOAR, para la automatización de la respuesta y el enriquecimiento de los eventos de seguridad.
  - Base de Datos de Inteligencia de Amenazas: Un repositorio actualizado de firmas de malware y TTPs para comparar el comportamiento observado.
  - Plataforma de Gestión y Monitoreo: Una consola centralizada para enviar muestras, visualizar los resultados y generar informes.
- ✓ **Requisitos y Alcances Técnicos**
- El proveedor debe garantizar que la solución cumpla con los siguientes requisitos:
- Procesamiento de Alto Rendimiento: La capacidad de analizar grandes volúmenes de archivos y URLs en poco tiempo para no afectar el flujo de la red.
  - Evasión de Sandbox: La plataforma debe ser capaz de detectar y neutralizar las técnicas de evasión utilizadas por el malware, como las verificaciones de entornos virtuales o la activación retardada.
  - Escalabilidad: El servicio debe ser escalable para manejar un aumento en el volumen de tráfico sin degradación del rendimiento.
  - Disponibilidad y Resiliencia: El servicio debe ofrecer alta disponibilidad con un acuerdo de nivel de servicio (SLA) que garantice un tiempo de actividad mínimo.
  - Privacidad y Encriptación: Los datos y archivos analizados deben estar cifrados en tránsito y en reposo.
- ✓ **Fabricantes y Soluciones en el Mercado**
- El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:
- Palo Alto Networks: Ofrece WildFire, una de las soluciones más avanzadas que se integra estrechamente con sus firewalls y la plataforma de seguridad.
  - Check Point: Su producto Threat Emulation proporciona un análisis de amenazas a gran escala y se integra con su arquitectura de seguridad.
  - Fortinet: FortiSandbox se integra con la suite de seguridad de la compañía, permitiendo el análisis de amenazas en tiempo real.

- Cisco: Su solución Cisco Secure Malware Analytics (anteriormente Threat Grid) ofrece un análisis de comportamiento detallado y reportes forenses.
- Kaspersky: Kaspersky Sandbox está diseñado para complementar sus soluciones de seguridad de endpoints.

#### ✓ **Funcionamiento del Servicio (Diagrama de Flujo)**

El proceso de un servicio de sandbox es secuencial y automatizado:

- Recepción del Objeto: Un archivo o URL sospechoso es recibido por un punto de entrada (email, firewall, endpoint).
- Envío a la Sandbox: El objeto es enviado automáticamente al entorno de sandbox para su análisis.
- Ejecución y Monitoreo: El objeto se ejecuta en el entorno virtual, mientras el sistema monitorea y registra cada una de sus acciones.
- Análisis de Comportamiento: El motor de sandbox analiza las acciones del objeto y las compara con bases de datos de amenazas conocidas.
- Generación de Veredicto: El sistema emite un veredicto de seguridad (benigno, sospechoso, malicioso).
- Acción de Respuesta: En caso de un veredicto malicioso, el sistema de seguridad se integra con otros componentes para bloquear el objeto, ponerlo en cuarentena o iniciar una respuesta automática.

#### ✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

❏ **MONITOREO Y CORRELACIÓN DE EVENTOS:** El servicio debe proporcionar monitoreo, detección y respuesta en tiempo real a las amenazas cibernéticas, asegurando la confidencialidad, integridad y disponibilidad de los activos de información. El sistema debe correlacionar eventos de seguridad de diversas fuentes para identificar ataques sofisticados y comportamientos anómalos.

#### ✓ **Elementos Mínimos para el Servicio de Ciberseguridad**

El servicio debe incluir, como mínimo, los siguientes elementos de hardware y software:

- Plataforma de Gestión de Eventos e Información de Seguridad (SIEM): Es la columna vertebral del servicio. Debe ser una solución robusta y escalable que centralice los registros (logs) de seguridad de todos los dispositivos y aplicaciones de la red.
- Gestor de Vulnerabilidades (Vulnerability Management): Herramienta que escanea y evalúa los sistemas para identificar vulnerabilidades.
- Estrategia de Inteligencia de Amenazas (Threat Intelligence): Bases de datos y flujos de información sobre amenazas emergentes, que se integran con el SIEM para una detección proactiva.

- Sistema de Detección de Intrusiones (IDS/IPS): Software o hardware que monitorea el tráfico de red para detectar actividad maliciosa.

#### ✓ **Funcionalidades del Servicio**

El servicio de ciberseguridad debe ofrecer las siguientes funcionalidades:

- Correlación de Eventos: Analiza y correlaciona los eventos de múltiples fuentes para identificar patrones de ataque que pasarían desapercibidos en un análisis individual.
- Análisis Forense: En caso de un incidente, el servicio debe permitir la investigación y el análisis detallado para determinar la causa raíz del ataque.
- Gestión de Incidentes: Proceso estructurado para la detección, contención, erradicación y recuperación de incidentes de seguridad.
- Generación de Informes: Debe proporcionar informes detallados sobre el estado de la seguridad, las amenazas detectadas y las acciones tomadas.

#### ✓ **Fabricantes y Requisitos Técnicos**

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son: Splunk, IBM QRadar, Microsoft Sentinel, LogRhythm o FortiSIEM. El proveedor debe contar con certificaciones en las tecnologías que ofrece.

- Capacidades de Integración: La plataforma debe ser capaz de integrarse con una amplia gama de dispositivos y aplicaciones, incluyendo firewalls, servidores, bases de datos y sistemas de nube.
- Escalabilidad: El sistema debe poder manejar el crecimiento del volumen de datos (logs) sin degradar el rendimiento.
- Arquitectura del Servicio: El servicio puede ser ofrecido en la nube, on-premise, o en un modelo híbrido, dependiendo de las necesidades de la compañía.

#### ✓ **Alcances y Pre-requisitos Técnicos**

Para una implementación exitosa, se deben cumplir los siguientes requisitos:

- Conectividad de Red: Se requiere una red estable para la transmisión segura de los logs de seguridad a la plataforma de monitoreo.
- Agentes de Monitoreo: Los servidores y dispositivos clave deben tener agentes de monitoreo instalados para recopilar logs de eventos.
- Política de Seguridad: Se debe definir una política de seguridad clara que establezca qué eventos deben ser monitoreados, cómo deben ser manejados y quién es responsable de la respuesta a incidentes.
- Personal Calificado: El proveedor debe contar con analistas de seguridad con experiencia en la operación y gestión de la plataforma de ciberseguridad.

#### ✓ **Consideraciones para la Seguridad y Disponibilidad**

Para garantizar que el servicio sea integral, seguro y disponible:

- Cifrado de Datos: Los datos deben ser cifrados tanto en tránsito como en reposo para proteger la información sensible.
- Alta Disponibilidad: El servicio debe contar con mecanismos de alta disponibilidad y redundancia para evitar interrupciones en el monitoreo.
- Respuesta a Incidentes: Se deben establecer protocolos de respuesta a incidentes que incluyan la comunicación, la contención y la remediación de amenazas de manera oportuna.

- Cumplimiento Normativo: El servicio debe cumplir con las normativas de seguridad aplicables (como GDPR, HIPAA, etc.).

#### ✓ Elementos mínimos de la gestión del servicio

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

- ▣ **SOAR (SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE):** el objetivo del SOAR es optimizar las operaciones del Centro de Operaciones de Seguridad (SOC) de la compañía, garantizando una respuesta integral, segura y disponible ante incidentes de ciberseguridad.

#### ✓ Elementos Mínimos del Servicio

La plataforma SOAR debe contar con los siguientes componentes esenciales para su funcionamiento:

- Motor de Orquestación: Debe ser capaz de integrar y coordinar acciones entre diferentes herramientas de seguridad (SIEM, EDR, Firewall, etc.) a través de APIs, scripts o conectores predefinidos.
- Gestión de Casos (Case Management): Un sistema centralizado para crear, gestionar y documentar incidentes de seguridad, permitiendo la asignación de tareas, el seguimiento del progreso y la colaboración entre analistas.
- Automatización de Playbooks (Playbook Automation): La capacidad de crear flujos de trabajo (playbooks) predefinidos que automatizan tareas manuales y repetitivas, como la triaje de alertas, la recolección de inteligencia de amenazas y la contención de incidentes.
- Panel de Control y Analíticas: Un dashboard intuitivo que proporcione una visión holística del estado de los incidentes, el rendimiento de los playbooks y métricas clave (KPIs), como el tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR).

#### ✓ Funcionalidades Detalladas

- Detección y Respuesta Automatizada: Debe permitir la automatización de la respuesta a incidentes comunes, como el bloqueo de IPs maliciosas, el aislamiento de endpoints comprometidos y la reinicialización de contraseñas.
- Inteligencia de Amenazas (Threat Intelligence): La capacidad de consumir y correlacionar feeds de inteligencia de amenazas para enriquecer la información de los incidentes y priorizar las alertas.
- Integración con Múltiples Fabricantes: La plataforma debe ser compatible con un amplio ecosistema de fabricantes de seguridad, como Palo Alto Networks, Fortinet, Check Point, Microsoft, y CrowdStrike, para garantizar una interoperabilidad fluida.
- Gestión de Vulnerabilidades: Debe integrarse con herramientas de escaneo de vulnerabilidades para automatizar la priorización y gestión de parches.

- Generación de Informes: La plataforma debe generar reportes personalizados sobre el estado de la seguridad, el rendimiento del SOC y la efectividad de las medidas de respuesta.

#### ✓ Prerrequisitos y Alcance Técnico

- Infraestructura: La solución debe ser compatible con entornos locales (on-premise) y en la nube (SaaS), garantizando la flexibilidad de la implementación.
- Integración de Datos: La plataforma SOAR debe poder consumir datos de un SIEM (ej. Splunk, IBM QRadar, Microsoft Sentinel) y otras fuentes relevantes, como firewalls, EDR, y sistemas de gestión de identidades.
- Requisitos de Conectividad: Se debe garantizar una conectividad segura y de alta velocidad entre la plataforma SOAR y las herramientas integradas para evitar latencia en la respuesta.
- Soporte y Mantenimiento: El proveedor debe ofrecer soporte técnico 24/7 y actualizaciones de software que garanticen la disponibilidad y la seguridad de la plataforma.

#### ✓ Funcionamiento y Componentes Específicos

El servicio de ciberseguridad SOAR se basa en tres pilares:

- Orquestación: La coordinación de tareas y la comunicación entre diferentes herramientas de seguridad para una respuesta más eficiente. Por ejemplo, un evento en el EDR (Endpoint Detection and Response) dispara una acción en el firewall.
- Automatización: La ejecución de tareas sin intervención humana.
- Respuesta (Response): La capacidad de tomar acciones decisivas ante una alerta, como la cuarentena de un archivo o la anulación de una cuenta de usuario.

El modelo de operación se centra en la creación de playbooks para los casos de uso más comunes, como:

- Phishing: El playbook analiza el correo, extrae URLs y archivos adjuntos, los somete a un sandbox, bloquea al remitente y notifica al usuario.
- Malware en Endpoint: El playbook aísla el endpoint de la red, escanea en busca de malware, y genera un informe de la amenaza.
- La implementación de la plataforma SOAR busca transformar el SOC de un modelo reactivo a uno proactivo y eficiente, reduciendo la carga de trabajo manual y mejorando la capacidad de respuesta ante amenazas.

#### ✓ Elementos mínimos de la gestión del servicio

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

- ▣ **NETWORK ACCESS CONTROL NAC:** La finalidad es fortalecer la postura de ciberseguridad, asegurando que solo los dispositivos y usuarios autorizados y que cumplan con las políticas de seguridad de la organización puedan acceder a la red. La solución debe ser integral, robusta y escalable, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

✓ **Alcance Técnico de la Solución NAC**

La solución NAC deberá gestionar y controlar el acceso a la red, tanto para los usuarios internos como para los invitados y dispositivos de terceros. El servicio debe ser capaz de:

- Identificar y Autenticar: Reconocer a los usuarios y dispositivos que intentan conectarse a la red.
- Autorizar: Aplicar políticas de acceso basadas en la identidad del usuario/dispositivo, su rol y el estado de seguridad de su equipo.
- Evaluar la Postura de Seguridad: Inspeccionar los dispositivos para verificar que cumplen con las políticas de la compañía (ej. tener el antivirus actualizado, el firewall activo, etc.).
- Segmentación Dinámica: Asignar automáticamente a los dispositivos a segmentos de red apropiados, limitando su acceso solo a los recursos necesarios.
- Remediación: Poner en cuarentena o bloquear a los dispositivos que no cumplan con las políticas, y guiarlos para que solucionen los problemas.

✓ **Componentes Mínimos para un Servicio de Ciberseguridad Integral**

Para que la solución NAC sea efectiva, deberá integrarse con los siguientes componentes de ciberseguridad:

- Autenticación Fuerte: Integración con un servicio de directorio centralizado (Active Directory, LDAP, etc.) y soporte para autenticación de dos o múltiples factores (MFA).
- Gestión de Vulnerabilidades: Conectividad con herramientas de escaneo de vulnerabilidades para evaluar el estado de los dispositivos.
- Firewalls y Sistemas de Detección/Prevención de Intrusiones (IDS/IPS): La solución NAC debe trabajar en conjunto con estos sistemas para aplicar políticas de seguridad.
- Antivirus/Antimalware Centralizado: La solución debe verificar el estado del software de seguridad de los endpoints.
- Gestión de Parches: La solución NAC debe ser capaz de verificar que los dispositivos tengan los parches de seguridad instalados.

✓ **Funcionalidades Detalladas y Requisitos Técnicos**

- Control de Acceso a la Red: La solución debe soportar el protocolo 802.1X para el control de acceso a nivel de puerto.
- Visibilidad de la Red: Debe proporcionar una vista completa de todos los dispositivos conectados a la red, incluyendo dispositivos IoT yBYOD (Bring Your Own Device).
- Integración de API: Capacidad para integrarse con soluciones de seguridad y TI de terceros a través de APIs (Interfaces de Programación de Aplicaciones).

- Gestión Centralizada: Una consola de gestión centralizada que permita la configuración de políticas, el monitoreo en tiempo real y la generación de informes detallados.
- Alta Disponibilidad: La solución debe ser redundante y tolerante a fallos para garantizar la operación continua.

✓ **Fabricantes Reconocidos en el mercado**

Se recomienda evaluar soluciones de fabricantes líderes en el mercado de NAC, tales como:

- Cisco Identity Services Engine (ISE): Una solución robusta y ampliamente utilizada, conocida por su integración con el ecosistema de Cisco.
- ClearPass Policy Manager (HPE Aruba): Ofrece flexibilidad y soporte para múltiples proveedores, ideal para entornos heterogéneos.
- Forescout Platform: Proporciona una visibilidad completa de todos los dispositivos conectados a la red y automatiza las políticas de control.
- Portnox CLEAR: Solución NAC basada en la nube, simplifica la implementación y la gestión para organizaciones de todos los tamaños.

✓ **Funcionamiento**

La solución NAC debe operar en un modelo de inspección y control en tiempo real:

- Conexión del Dispositivo: Un dispositivo intenta conectarse a la red.
- Autenticación: El AP o el switch envía la solicitud al servidor NAC para autenticar al dispositivo y/o al usuario.
- Evaluación de la Postura: El NAC realiza una evaluación del dispositivo para verificar que cumpla con las políticas de seguridad.
- Autorización: El NAC autoriza o deniega el acceso, o lo pone en cuarentena si no cumple con las políticas.
- Segmentación: El dispositivo autorizado es asignado a la VLAN y al segmento de red adecuados.
- Monitoreo Continuo: El NAC monitorea el dispositivo para asegurar que mantenga su estado de seguridad mientras está conectado a la red.

✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

- **PAM:** solución de ciberseguridad está diseñada para controlar, monitorear y gestionar las cuentas con privilegios en una organización. Estas cuentas, que incluyen a administradores de sistemas, desarrolladores y personal de TI, tienen acceso a información y sistemas críticos, lo que las convierte en un objetivo principal para los ciberataques. La funcionalidad del PAM se centra en mitigar los riesgos asociados con el abuso de estos accesos.

✓ **Las funcionalidades esperadas para la solución PAM son:**

- Bóveda de Contraseñas (Password Vaulting): Almacena de forma centralizada y segura las credenciales de las cuentas privilegiadas. Las contraseñas se gestionan y rotan automáticamente para evitar su uso indebido.
- Gestión de Sesiones (Session Management): Controla y monitorea en tiempo real las sesiones de acceso privilegiado. Esto permite a los administradores supervisar las actividades de los usuarios y, si es necesario, terminar una sesión sospechosa.
- Gestión de Privilegios (Privilege Elevation): Permite a los usuarios obtener acceso privilegiado solo cuando lo necesitan (Just-in-Time Access), minimizando el riesgo de uso no autorizado de privilegios.
- Auditoría y Monitoreo: Registra todas las actividades realizadas durante una sesión privilegiada. Estos registros son cruciales para la auditoría, el análisis forense y el cumplimiento de normativas.

✓ **Alcances Técnicos y Requisitos del Servicio**

El alcance de una solución PAM debe ser integral para proteger toda la infraestructura de la organización. Los requisitos mínimos para un servicio de PAM incluyen:

- Inventario y Descubrimiento: La solución debe ser capaz de identificar automáticamente todas las cuentas privilegiadas en la red, incluyendo servidores, bases de datos y dispositivos de red.
- Control de Acceso: Debe implementar un control de acceso basado en el menor privilegio, permitiendo a los usuarios acceder solo a los recursos que necesitan para su trabajo.
- Autenticación: Debe integrar la autenticación multifactor (MFA) para todas las cuentas privilegiadas.
- Seguridad y Cifrado: Los datos almacenados en la bóveda de contraseñas deben estar cifrados en reposo y en tránsito.
- Integración: La solución debe ser compatible con la infraestructura de TI existente, incluyendo directorios de usuarios (como Active Directory o LDAP), sistemas SIEM (Gestión de Información y Eventos de Seguridad) y herramientas de gestión de identidad.
- Disponibilidad y Resiliencia: La solución debe ser altamente disponible, con mecanismos de redundancia y recuperación ante desastres para garantizar que el servicio esté siempre operativo.

✓ **Componentes Específicos para un Servicio de Ciberseguridad Integral**

Para que un servicio de PAM sea realmente integral, debe ser parte de un ecosistema de ciberseguridad más amplio. Los componentes adicionales que se deben incluir son:

- Identificación y Acceso de Identidad (IAM): El IAM gestiona la identidad y el acceso de los usuarios regulares. El PAM complementa el IAM al centrarse exclusivamente en las cuentas privilegiadas.
- Plataformas de Ciberseguridad: La solución PAM debe integrarse con herramientas como firewalls de próxima generación, sistemas de detección de intrusiones (IDS) y antivirus para una defensa en profundidad.

- SIEM (Gestión de Información y Eventos de Seguridad): Un SIEM recopila y analiza los registros del PAM, permitiendo la detección de amenazas y anomalías en tiempo real.
- Monitoreo Continuo: Se debe establecer un monitoreo 24/7 para detectar actividades sospechosas en las cuentas privilegiadas.

#### ✓ **Fabricantes y Pre-requisitos**

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- CyberArk: Considerado líder en el mercado de PAM. Ofrece un conjunto completo de funcionalidades que van más allá del PAM básico, incluyendo la gestión de privilegios para la nube y DevOps.
- BeyondTrust: Un competidor fuerte que ofrece una plataforma unificada para la gestión de accesos privilegiados, que incluye la gestión de contraseñas y el control de acceso remoto.
- Delinea (antes Thycotic): Provee soluciones fáciles de implementar y gestionar, ideal para organizaciones que buscan una solución rápida y eficiente.
- IBM

#### ✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

☐ **IAM:** Este servicio debe asegurar que solo los usuarios autorizados (empleados, clientes, socios) tengan acceso a los recursos digitales apropiados (aplicaciones, sistemas, datos), en el momento correcto y por la razón correcta. El objetivo principal es reducir el riesgo de acceso no autorizado y simplificar la gestión de identidades en todo el ecosistema de TI.

#### ✓ **Elementos Mínimos y Alcances Técnicos**

El servicio de IAM debe incluir, como mínimo, las siguientes funcionalidades y componentes:

- Gestión Centralizada de Identidades: Un repositorio central para todas las identidades digitales. Debe permitir la creación, modificación y eliminación de usuarios y sus perfiles de forma unificada.
- Autenticación Fuerte:
  - Autenticación Multifactor (MFA): La solución debe ser compatible con múltiples métodos de autenticación, como códigos de un solo uso (OTP), biometría, tokens de seguridad (hardware y software), y aplicaciones de autenticación.
  - Inicio de Sesión Único (SSO): Los usuarios deben poder acceder a múltiples aplicaciones y servicios con un solo conjunto de credenciales.

- **Gestión de Acceso:**
  - **Control de Acceso Basado en Roles (RBAC):** El acceso a los recursos debe basarse en los roles y responsabilidades de los usuarios dentro de la organización, no en sus identidades individuales.
  - **Acceso con Privilegios Mínimos:** La solución debe garantizar que los usuarios solo tengan los permisos necesarios para realizar sus tareas, reduciendo el riesgo de abuso.
- **Gestión del Ciclo de Vida del Acceso:** Debe automatizar la creación de cuentas para los nuevos empleados, la modificación de permisos para los cambios de rol y la desactivación de cuentas para las bajas laborales.
- **Auditoría y Monitoreo:** La solución debe registrar y auditar todas las actividades de acceso (quién accedió a qué recurso, cuándo y desde dónde). Esta información es crucial para el cumplimiento normativo y para la detección de anomalías.

#### ✓ **Funcionamiento**

El servicio de IAM funcionará como un punto de control centralizado. Cuando un usuario intente acceder a una aplicación o recurso, el sistema de IAM verificará su identidad y sus permisos. Si la identidad es válida y el usuario tiene los permisos requeridos, se le otorgará el acceso. Este proceso es transparente para el usuario final gracias a la implementación del SSO.

- **Identificación:** El usuario se identifica.
- **Autenticación:** El sistema verifica la identidad del usuario, preferiblemente con MFA.
- **Autorización:** El sistema de RBAC verifica los permisos del usuario para el recurso solicitado.
- **Auditoría:** Todas las interacciones se registran para su posterior análisis.

#### ✓ **Fabricantes y Soluciones**

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- m) **Microsoft:** Con su suite Azure Active Directory (ahora Entra ID), que ofrece una solución completa para la nube y entornos híbridos.
- n) **Okta:** Líder en soluciones de SSO y MFA, con un enfoque en la experiencia del usuario y la integración con miles de aplicaciones.
- o) **Ping Identity:** Ofrece una plataforma integral de seguridad de identidad para la empresa.
- p) **ForgeRock:** Proporciona una plataforma de identidad de código abierto.
- q) **CyberArk:** Especializado en la Gestión de Acceso Privilegiado (PAM), una capa crítica de IAM.

#### ✓ **Requisitos y Componentes Específicos**

- **Disponibilidad y Resiliencia:** La solución debe ofrecer una alta disponibilidad (99.9% o superior) y ser redundante, con capacidades de recuperación ante desastres para garantizar la continuidad del servicio.
- **Seguridad y Cifrado:** Todas las comunicaciones y los datos de identidad deben estar cifrados tanto en tránsito como en reposo. Se debe cumplir con los estándares de seguridad como NIST o ISO 27001.

- Integración: La solución debe ser compatible y poder integrarse fácilmente con las aplicaciones existentes de la compañía, ya sean locales, en la nube o SaaS.
  - Escalabilidad: El sistema debe ser capaz de escalar para manejar un número creciente de usuarios, dispositivos y aplicaciones.
  - Reportes y Analíticas: Se requiere la capacidad de generar reportes detallados y analíticas para la auditoría, la detección de amenazas y la toma de decisiones.
- ✓ **Elementos mínimos de la gestión del servicio**  
El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:
- Hardware/Software de última generación.
  - Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
  - Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
  - Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.
- ☐ **Agente de Seguridad de Acceso a la Nube (CASB):** diseñado para unificar y fortalecer la ciberseguridad en entornos de nube. Este documento cubre los elementos mínimos, funcionalidades, fabricantes, requisitos, alcances y el funcionamiento para garantizar un servicio integral, seguro y disponible. La adopción de servicios en la nube (SaaS, IaaS, PaaS) por parte de la organización ha generado una dispersión de datos y una reducción en la visibilidad y el control de la seguridad. El **CASB (Cloud Access Security Broker)** es un componente crítico que actúa como un punto de control de seguridad entre los usuarios y los proveedores de servicios en la nube. Su implementación es esencial para extender las políticas de seguridad corporativas a la nube, mitigar riesgos de fugas de datos y proteger contra amenazas avanzadas.
- ✓ **Requisitos y Alcances Técnicos del Servicio**  
El servicio de CASB debe ser provisto como una solución gestionada, con las siguientes características técnicas y alcances mínimos:
- m) Funcionalidades de Seguridad Requeridas**  
El CASB debe operar en los cuatro pilares fundamentales definidos por Gartner: visibilidad, seguridad de datos, protección contra amenazas y cumplimiento normativo.
- ✓ **Visibilidad y Control (Shadow IT):**
- Descubrimiento de Aplicaciones: Debe tener la capacidad de identificar y clasificar todas las aplicaciones en la nube, tanto las aprobadas (sancionadas) como las no autorizadas (Shadow IT), utilizadas por los usuarios de la organización. Esto incluye la evaluación de su nivel de riesgo.
  - Monitoreo del Tráfico: Debe monitorear en tiempo real el tráfico de usuarios hacia los servicios de nube, incluso en conexiones cifradas con SSL/TLS.
- ✓ **Seguridad de Datos (Data Loss Prevention - DLP):**

- Clasificación de Datos: Debe clasificar los datos sensibles (información personal, financiera, propiedad intelectual) para aplicar políticas de seguridad.
  - Prevención de Fuga de Datos (DLP): Debe prevenir la carga, descarga o el compartir de archivos que contengan información sensible fuera de la red corporativa. Esto debe ser configurable con políticas granulares.
  - Encriptación: Debe ofrecer capacidades de encriptación de datos en tránsito y en reposo en la nube para asegurar la confidencialidad.
- ✓ **Protección contra Amenazas (Threat Protection):**
- Detección de Malware: Debe escanear en tiempo real los archivos subidos y descargados de la nube para detectar y bloquear malware, ransomware y otras amenazas.
  - Análisis de Comportamiento (UEBA): Debe utilizar análisis de comportamiento de usuarios y entidades (UEBA) para detectar anomalías, como inicios de sesión desde ubicaciones inusuales o descargas masivas de datos, que puedan indicar cuentas comprometidas o amenazas internas.
- ✓ **Cumplimiento Normativo (Compliance):**
- Auditoría y Reportes: Debe generar informes detallados para demostrar el cumplimiento de normativas como HIPAA, GDPR, PCI DSS y otras regulaciones aplicables.
  - Aplicación de Políticas: Debe asegurar que las políticas de seguridad se apliquen de manera consistente en todos los servicios de nube utilizados.
- ✓ **Opciones de Despliegue y Funcionamiento**  
El proveedor debe ofrecer las siguientes opciones de despliegue para adaptarse a las necesidades de la organización:
- h. Implementación Basada en API:**
- v. Descripción: La solución se integra directamente con las APIs de los servicios en la nube (como Microsoft 365, Google Workspace, Salesforce). Esto permite un control total sobre los datos "en reposo" y sobre las actividades de los usuarios.
  - vi. Ventajas: Ofrece una visibilidad profunda del uso de la aplicación y el contenido almacenado, y no interfiere con el flujo de tráfico del usuario.
- i. Implementación Basada en Proxy:**
- Descripción: El tráfico de red se redirige a través del CASB (como un proxy inverso o directo).
  - Ventajas: Permite un control en tiempo real sobre las actividades y los datos en tránsito, lo que es ideal para prevenir la carga de archivos maliciosos o el uso de Shadow IT.
- ✓ **Elementos Mínimos del Servicio**  
Para garantizar una solución integral, segura y disponible, el servicio debe incluir los siguientes elementos:
- Soporte del Fabricante: Se requiere que el servicio y todos sus componentes técnicos cuenten con soporte directo y garantizado del fabricante durante toda

la vigencia del contrato, con acuerdos de nivel de servicio (SLA) definidos para tiempos de respuesta y resolución de incidentes.

- Capacidades de Integración: La solución debe integrarse de forma nativa con el IdP (Identity Provider) de la organización (ej. Active Directory, SAML 2.0) para el control de acceso y la autenticación. También debe ser compatible con soluciones de SIEM/SOAR para la correlación de eventos y la automatización de respuestas.
- Monitoreo y Gestión: El proveedor debe ofrecer una plataforma de monitoreo y gestión centralizada que permita la supervisión en tiempo real, la generación de alertas y la administración de políticas de seguridad.
- Reportes y Analíticas: El servicio debe incluir un motor de reportes con la capacidad de generar informes detallados y personalizados sobre la actividad de los usuarios, el cumplimiento, el uso de aplicaciones y las amenazas detectadas.
- Modelo de Licenciamiento: El licenciamiento debe ser flexible y escalable, preferiblemente por usuario o por la cantidad de datos gestionados, para ajustarse al crecimiento de la organización.

#### ✓ Fabricantes y Proveedores (Ejemplos)

Existen varios fabricantes líderes en el mercado de CASB, entre los que se destacan:

- Palo Alto Networks (Prisma Access): Conocido por su enfoque de seguridad integral y su integración con su plataforma SASE.
- Netskope: Uno de los líderes del mercado, reconocido por su arquitectura nativa de la nube y sus capacidades de inspección profunda de datos.
- Forcepoint: Ofrece una plataforma de seguridad convergente, con fuertes capacidades de protección de datos y DLP.
- McAfee Enterprise (MVISION Cloud): Proporciona seguridad de datos y control de amenazas en múltiples servicios de nube.
- Zscaler: Con su solución Zscaler Cloud Protection, se enfoca en la seguridad de la nube a través de una arquitectura SASE.

#### ✓ Elementos mínimos de la gestión del servicio

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

- **Secure Access Service Edge (SASE):** es un modelo de arquitectura de red que integra capacidades de red de área extensa (WAN) con servicios de seguridad integrales. SASE es una solución basada en la nube. Combina las pasarelas seguras de Web, el corredor de seguridad de acceso a la nube, el cortafuegos como servicio y el acceso a la red de confianza cero. Todos estos componentes están unificados en un solo sistema. Esta convergencia permite una aplicación coherente de la seguridad y un rendimiento óptimo, proporcionando a los usuarios

un acceso seguro y sin fisuras a las aplicaciones y los datos, independientemente de su ubicación.

### ✓ Elementos Mínimos del Servicio SASE

Un servicio SASE debe converger las capacidades de red y seguridad en una única plataforma basada en la nube. Los componentes mínimos requeridos son:

- SD-WAN (Software-Defined Wide Area Network): Componente de red que optimiza la conectividad, dirigiendo el tráfico de manera inteligente a través de múltiples enlaces (MPLS, internet de banda ancha, 4G/5G). Su función es asegurar un rendimiento óptimo de las aplicaciones y la resiliencia de la conexión.
- SWG (Secure Web Gateway): Sirve como una puerta de enlace segura para el tráfico web. Inspecciona y filtra el tráfico de internet para proteger a los usuarios de amenazas basadas en la web, como malware, phishing y sitios web maliciosos.
- FWaaS (Firewall as a Service): Un firewall que se ofrece como un servicio en la nube, eliminando la necesidad de hardware físico. Proporciona capacidades de firewall de última generación (NGFW) como el filtrado de URL, la prevención de intrusiones y el control de aplicaciones.
- ZTNA (Zero Trust Network Access): Un modelo de seguridad que opera bajo el principio de "nunca confíes, siempre verifica". A diferencia de una VPN, ZTNA otorga acceso granular a aplicaciones específicas en lugar de a toda la red, basándose en la identidad del usuario y el estado del dispositivo.
- CASB (Cloud Access Security Broker): Proporciona visibilidad y control sobre el uso de aplicaciones en la nube (SaaS). Ayuda a proteger los datos sensibles, prevenir fugas de información y garantizar el cumplimiento de las políticas de seguridad en la nube.

### ✓ Funcionalidades y Alcances Técnicos

El servicio SASE debe ir más allá de la simple agregación de componentes, ofreciendo un conjunto de funcionalidades integradas para una seguridad robusta y una experiencia de usuario optimizada:

- Identidad y Control de Acceso: La seguridad se basa en la identidad del usuario y del dispositivo, no en la dirección IP. El sistema debe integrarse con proveedores de identidad (como Active Directory) y usar autenticación multifactor (MFA) para validar el acceso.
- Inspección de Tráfico Encriptado: Capacidad para descifrar y volver a cifrar el tráfico SSL/TLS para una inspección profunda y la detección de amenazas ocultas.
- Prevención de Pérdida de Datos (DLP): Funcionalidad para identificar y evitar la fuga de información sensible, aplicando políticas de protección de datos en todos los puntos de la red.
- Visibilidad y Monitoreo Centralizado: Una plataforma de gestión unificada que brinde una visibilidad completa del tráfico de red y de las actividades de los usuarios. Debe incluir herramientas de análisis e informes para la detección de anomalías y la respuesta a incidentes.
- Seguridad impulsada por IA/ML: Uso de algoritmos de inteligencia artificial y machine learning para la detección proactiva de amenazas, el análisis del

comportamiento de los usuarios (UEBA) y la automatización de la respuesta a incidentes.

#### ✓ **Fabricantes y Soluciones**

El mercado de SASE está dominado por proveedores que ofrecen soluciones "de un solo proveedor" o plataformas consolidadas. Algunos de los principales fabricantes son:

- Zscaler: Conocido por su enfoque de seguridad centrado en la nube y su plataforma Zscaler Private Access (ZPA) para ZTNA.
- Palo Alto Networks: Su solución Prisma SASE integra sus firewalls de próxima generación con capacidades de SD-WAN y seguridad en la nube.
- Fortinet: FortiSASE se beneficia de su amplio "Security Fabric" para ofrecer una solución integrada de red y seguridad.
- Cisco: Ofrece su solución con Cisco+ Secure Connect, aprovechando su herencia en redes y su portafolio de seguridad.
- Netskope: Se destaca por su liderazgo en seguridad de aplicaciones en la nube (CASB).
- Cato Networks: Es un pionero en la arquitectura SASE, ofreciendo una plataforma unificada y nativa de la nube.

#### ✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

❏ **FIREWALL BASE DE DATOS:** es un componente de seguridad que opera como un dispositivo de seguridad o software de monitoreo y control para el tráfico de red dirigido a las bases de datos. Su principal objetivo es proteger los datos sensibles de amenazas internas y externas.

Su funcionalidad se centra en:

- Monitoreo del Tráfico: Inspecciona y analiza todo el tráfico de red, incluyendo las consultas SQL, para identificar actividades anómalas o sospechosas.
- Prevención de Intrusiones: Bloquea ataques de inyección SQL, abusos de privilegios y accesos no autorizados a la base de datos en tiempo real.
- Auditoría y Conformidad: Registra cada consulta y actividad del usuario, proporcionando una pista de auditoría completa para cumplir con normativas como PCI-DSS, GDPR o SOX.
- Protección de Datos Sensibles: Identifica y clasifica los datos confidenciales, aplicando políticas de seguridad para evitar su exfiltración o modificación no autorizada.

#### ✓ **Elementos Mínimos del Servicio**

Un servicio de ciberseguridad integral no solo incluye el firewall, sino que también se apoya en otros componentes para garantizar su efectividad:

- Sonda de Monitoreo (Database Activity Monitoring - DAM): Es una herramienta que captura y audita cada transacción, incluso si el tráfico está cifrado, y genera alarmas en tiempo real.
- Motor de Análisis de Vulnerabilidades: Un componente que escanea la base de datos en busca de vulnerabilidades, configuraciones incorrectas y fallas de seguridad.
- Sistema de Gestión y Correlación de Eventos (SIEM): Recopila los logs del firewall y de otros sistemas, los correlaciona para detectar patrones de ataque complejos y proporciona una visión unificada de la seguridad.

#### ✓ Alcances y Requisitos Técnicos

Para que el servicio sea efectivo, se deben definir los siguientes alcances:

- Alcance de Cobertura: El firewall debe proteger bases de datos en entornos On-Premise, en la nube (DBaaS) o en entornos híbridos.
- Soporte de Bases de Datos: Debe ser compatible con las bases de datos más comunes como Oracle, Microsoft SQL Server, MySQL, PostgreSQL y MongoDB.
- Integración con SIEM: Debe poder enviar los logs y las alertas a un sistema SIEM para una gestión centralizada de la seguridad.
- Soporte de Encriptación: Debe poder inspeccionar el tráfico incluso si la conexión está encriptada, ya sea a través de la instalación de certificados o con la terminación del cifrado.

#### ✓ Funcionamiento y Configuración

El firewall de base de datos funciona en dos modos principales:

- Modo de Monitoreo (Pasivo): El firewall analiza el tráfico sin bloquearlo. Es útil para auditar el tráfico y crear una línea base de actividad normal.
- Modo de Prevención (Activo): El firewall bloquea automáticamente las consultas y las conexiones que considera maliciosas, protegiendo la base de datos de ataques en tiempo real.
- Las configuraciones clave incluyen:
- Políticas de Seguridad: Reglas que definen qué tipo de tráfico se permite y qué se bloquea.
- Clasificación de Datos: Reglas que identifican los datos sensibles (por ejemplo, números de tarjetas de crédito o información personal) y les aplican medidas de protección.
- Control de Privilegios: Restricciones a los comandos SQL que pueden ejecutar ciertos usuarios.

#### ✓ Fabricantes y Soluciones

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- Imperva: Con su producto Imperva Database Security, es uno de los líderes del mercado, conocido por su sólida protección contra amenazas y su cumplimiento normativo.

- Oracle Audit Vault and Database Firewall: Una solución de Oracle que se integra de manera nativa con sus bases de datos, ofreciendo una protección robusta y herramientas de auditoría.
- McAfee Database Security: Ofrece un conjunto de herramientas para la seguridad de bases de datos, incluyendo monitoreo de actividad, análisis de vulnerabilidades y prevención de intrusiones.
- IBM Guardium: Una solución integral que proporciona descubrimiento, monitoreo de actividad, análisis de vulnerabilidades y encriptación de datos.

✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

☐ **GESTIÓN DE CONTRASEÑAS (Password Manager):** debe ser una solución de ciberseguridad robusta y centralizada para la administración segura de credenciales de acceso. Su objetivo principal es fortalecer la postura de seguridad de la organización al mitigar los riesgos asociados a contraseñas débiles, reutilizadas o almacenadas de forma insegura. La solución debe ser de grado empresarial y proveer funcionalidades avanzadas para la gestión de usuarios, la automatización y la auditoría.

✓ **El alcance técnico debe cubrir:**

- Gestión de Cuentas Privilegiadas (PAM - Privileged Access Management): La solución debe ser capaz de gestionar cuentas de alto riesgo, como las de administradores de sistemas y bases de datos.
- Control de Acceso a Contraseñas: Debe permitir un control granular sobre quién puede acceder a qué contraseñas, con base en roles y permisos predefinidos.
- Generación de Contraseñas Seguras: Debe tener la capacidad de generar automáticamente contraseñas complejas y únicas.
- Almacenamiento Cifrado: Todas las contraseñas y datos sensibles deben ser almacenados en una bóveda digital cifrada.

✓ **Funcionalidades Mínimas Requeridas**

- Autenticación Fuerte: Soporte para Autenticación Multifactor (MFA), incluyendo tokens de hardware, SMS, o aplicaciones de autenticación.
- Integración con Directorios: Capacidad de integrarse con servicios de directorio como Active Directory (AD) o LDAP para una gestión de usuarios centralizada y eficiente.
- Auditoría y Monitoreo: Debe ofrecer un registro completo de auditoría que documente el acceso a cada contraseña, permitiendo la trazabilidad y el análisis forense en caso de un incidente.

- Acceso Seguro: Capacidad de iniciar sesión automáticamente en aplicaciones y servicios sin exponer la contraseña al usuario. Esto debe incluir extensiones para navegadores y aplicaciones de escritorio.
- Monitoreo de la Oscuridad (Dark Web): El servicio debe ofrecer monitoreo de credenciales comprometidas en la dark web y alertar a los administradores en tiempo real.
- Flujos de Trabajo de Aprobación: Debe permitir la configuración de flujos de trabajo para que el acceso a contraseñas de alta seguridad requiera la aprobación de un administrador.

#### ✓ Requisitos Técnicos y Pre-requisitos

- Arquitectura: La solución puede ser on-premise (en los servidores de la compañía) o SaaS (gestionada en la nube). La arquitectura debe ser escalable para acomodar el crecimiento futuro de la organización.
- Soporte de Plataformas: Compatibilidad con los principales sistemas operativos (Windows, macOS, Linux), navegadores (Chrome, Firefox, Edge) y dispositivos móviles (iOS, Android).
- Cumplimiento Normativo: La solución debe estar certificada para cumplir con estándares de seguridad como ISO 27001, NIST o SOC 2.
- Integraciones API: Debe ofrecer una API (Interfaz de Programación de Aplicaciones) robusta para la integración con otras herramientas de seguridad y de TI.

#### ✓ Fabricantes y Soluciones Típicas

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- LastPass Enterprise: Conocido por su facilidad de uso y amplias funcionalidades.
- Dashlane Business: Se destaca por su interfaz intuitiva y funcionalidades de monitoreo de seguridad.
- Keeper Security: Ofrece una solución robusta con fuertes capacidades de gestión de acceso privilegiado (PAM).
- 1Password Business: Muy popular por su facilidad de uso y sus sólidas características de seguridad.
- CyberArk: Un líder del mercado en el espacio de PAM, ideal para organizaciones con estrictos requisitos de seguridad.

#### ✓ Funcionamiento y Componentes

El funcionamiento de un gestor de contraseñas integral se basa en varios componentes clave:

- Bóveda de Contraseñas Cifrada: Un contenedor digital donde todas las contraseñas son almacenadas de manera segura. Solo puede ser desbloqueado con una "contraseña maestra" y/o autenticación multifactor.
- Consola de Administración Centralizada: Permite a los administradores gestionar usuarios, roles, políticas de seguridad y auditar la actividad.
- Agentes de Escritorio y Móviles: Aplicaciones que se instalan en los dispositivos de los usuarios para facilitar el acceso seguro a las contraseñas y la sincronización con la bóveda central.

- Servidor de Almacenamiento y Sincronización: En el caso de soluciones on-premise, este es el servidor que aloja la bóveda cifrada y se encarga de la sincronización de datos.

#### ✓ Consideraciones de Seguridad y Disponibilidad

- Cifrado de Extremo a Extremo: Los datos deben estar cifrados en el dispositivo del usuario antes de ser enviados a la bóveda. Esto asegura que solo el usuario puede descifrarlos.
- Disponibilidad: La solución debe ofrecer un Acuerdo de Nivel de Servicio (SLA) que garantice una alta disponibilidad, idealmente superior al 99.9%.
- Respaldo y Recuperación: El proveedor debe tener políticas de respaldo y recuperación de datos sólidas para evitar la pérdida de información en caso de una falla.

#### ✓ Elementos mínimos de la gestión del servicio

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

☐ **INTELIGENCIA DE AMENAZAS (Threat Intelligence Service):** es un componente crítico de la ciberseguridad, diseñado para recolectar, procesar y analizar información sobre amenazas potenciales o existentes. Su objetivo es proporcionar datos procesables que permitan a las organizaciones anticipar, prevenir y responder a los ciberataques de manera proactiva. Este servicio va más allá de la detección de amenazas; su enfoque es estratégico y basado en el conocimiento.

#### ✓ Elementos Mínimos del Servicio de Inteligencia de Amenazas

Un servicio de inteligencia de amenazas integral debe incluir los siguientes componentes:

- Fuentes de Datos (Feeds): El servicio debe alimentarse de una amplia gama de fuentes, incluyendo bases de datos de vulnerabilidades (CVE), indicadores de compromiso (IoC), listas de direcciones IP maliciosas, dominios de phishing y telemetría de amenazas globales.
- Plataforma de Procesamiento: Un sistema que recolecta, normaliza y enriquece los datos de las fuentes. Esta plataforma debe utilizar algoritmos de Inteligencia Artificial (IA) y Aprendizaje Automático (Machine Learning) para identificar patrones, correlacionar eventos y generar alertas de alta fidelidad.
- Análisis y Contextualización: El servicio debe proporcionar un equipo de analistas de seguridad que contextualice los datos sin procesar, identificando a

los actores de amenazas (por ejemplo, grupos de APT), sus tácticas, técnicas y procedimientos (TTPs).

- Integración: La plataforma debe tener la capacidad de integrarse con los sistemas de seguridad existentes de la organización, como SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), firewalls y plataformas SOAR (Security Orchestration, Automation and Response).

#### ✓ **Funcionalidades y Alcances Técnicos**

El servicio debe ofrecer las siguientes funcionalidades clave:

- Inteligencia Estratégica: Proporciona una visión a largo plazo de las tendencias de amenazas, ayudando a la organización a tomar decisiones de seguridad informadas a nivel directivo.
- Inteligencia Táctica: Ofrece información sobre las TTPs de los atacantes, permitiendo a los equipos de seguridad fortalecer las defensas y mejorar los controles de seguridad.
- Inteligencia Operacional: Suministra datos específicos y procesables, como IoC, que pueden ser usados para la detección y bloqueo automático de amenazas en tiempo real.
- Alertas Personalizadas: Las notificaciones deben ser relevantes para el sector y la infraestructura de la compañía, evitando el "ruido" y las alertas falsas.
- Análisis de Vulnerabilidades: El servicio debe identificar las vulnerabilidades en los sistemas de la organización y priorizar cuáles deben ser parchadas primero basándose en el riesgo real que representan.
- Algoritmos de búsqueda y recolección automatizada (Robots) en redes sociales y otras fuentes de OSINT incluyendo todas las fuentes más conocidas Facebook, Twitter, YouTube, Instagram, Vkontakte, Tiktok, Pinterst, Weibo, Gab, Mastodon, Pastebin, Reddit, 4Chan, Telegram, Viber, Skype, WhatsApp, Trucaller, CallApp, Pipl\_Search, Whois Domain, Blockchain,
- Algoritmos Surface web: Motores de búsqueda, Páginas de Web, RSS,
- DarkNet: motores de búsqueda, páginas web entre otras.
- Para el caso de las redes sociales analizar comentarios, reacciones.
  - Conexiones (incluso si el objetivo tiene una lista de amigos cerrados).
  - Acerca de (grupos, páginas).
  - Ubicación del usuario.
  - Seguidores.
  - Imágenes etiquetadas por otros usuarios.
  - Historias destacadas (Stories y Highlights)

#### ✓ **Fabricantes y Proveedores**

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- FireEye (ahora Mandiant): Conocido por su inteligencia sobre APT (Advanced Persistent Threats).
- CrowdStrike: Ofrece una plataforma unificada que integra inteligencia de amenazas con protección de endpoints.
- Palo Alto Networks: Proporciona inteligencia de amenazas a través de su plataforma Unit 42.

- Recorded Future: Se especializa en inteligencia de amenazas predictiva y contextualizada.
- Kaspersky: Conocido por su vasta base de datos de amenazas globales.

#### ✓ **Pre-requisitos y Requisitos Operativos**

Para implementar el servicio, se requieren los siguientes pre-requisitos:

- Disponibilidad de Datos: La organización debe tener la capacidad de compartir logs y telemetría de sus dispositivos de seguridad con la plataforma de inteligencia de amenazas de forma segura.
- Personal Capacitado: Se necesita un equipo de seguridad (SOC) con el conocimiento necesario para interpretar y actuar sobre las alertas y los informes de inteligencia.
- Infraestructura de Integración: Se debe contar con la infraestructura necesaria para integrar el servicio con los sistemas de seguridad existentes a través de APIs, STIX/TAXII u otros protocolos estándar de la industria.

#### ✓ **Funcionamiento y Disponibilidad**

El funcionamiento del servicio debe ser un ciclo continuo y automatizado:

- Colección de Datos: La plataforma recolecta datos de las fuentes en tiempo real.
- Análisis: El sistema procesa los datos para identificar patrones y correlacionar eventos.
- Generación de Alertas: Se emiten alertas procesables y se envían a los sistemas de seguridad de la organización.
- Acción: Los equipos de seguridad utilizan la información para bloquear amenazas, actualizar firewalls y priorizar vulnerabilidades.
- La disponibilidad del servicio debe ser alta, con un SLA (Service Level Agreement) que garantice un tiempo de actividad del 99.9% o superior, y con un sistema de soporte 24/7 para responder a incidentes críticos.

#### ✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- Hardware/Software de última generación.
- Licenciamiento: Incluir todas las licencias necesarias para las funcionalidades requeridas.
- Soporte y Mantenimiento: Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- Monitoreo y Gestión: Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

☐ **BORRADO SEGURO:** es un proceso técnico y controlado para la eliminación irreversible de información almacenada en dispositivos de almacenamiento. A diferencia del formateo o la eliminación de archivos, el borrado seguro garantiza que los datos no puedan ser recuperados ni reconstruidos, cumplimiento con los estándares de seguridad y normativas de privacidad.

#### ✓ **Elementos Mínimos de Ciberseguridad**

Para que este servicio sea integral, seguro y disponible, debe contar con los siguientes elementos:

- Software de Borrado Seguro: El software debe estar certificado por organizaciones internacionales como el Instituto Nacional de Estándares y Tecnología (NIST) o la Agencia de Seguridad Nacional (NSA). Debe ser capaz de sobrescribir los datos con patrones específicos, asegurando su completa ilegibilidad.
- Hardware Específico: Equipos que garanticen el borrado seguro a nivel físico. Se debe usar hardware especializado para la desmagnetización (Degaussing) de medios magnéticos o la destrucción física de discos duros y unidades de estado sólido.
- Gestión de Logs y Auditoría: El sistema debe generar un registro detallado de cada proceso de borrado, incluyendo información como el número de serie del dispositivo, la fecha y hora del borrado, el método utilizado y el resultado final. Estos logs son cruciales para la auditoría y el cumplimiento normativo.
- Seguimiento de la Cadena de Custodia: Se debe implementar un protocolo estricto para rastrear los dispositivos desde su recepción hasta su destrucción o borrado.

#### ✓ Funcionalidades y Requisitos

- Borrado a Múltiples Niveles: El servicio debe ofrecer la eliminación de datos en varios niveles, incluyendo a nivel de archivo individual, partición de disco y borrado completo del dispositivo.
- Métodos de Borrado: Se deben utilizar algoritmos de borrado reconocidos, como DoD 5220.22-M, NIST SP 800-88 o Schneier. Estos métodos sobrescriben los datos varias veces con patrones aleatorios y específicos.
- Detección de Errores: El sistema debe validar que cada sector de un disco ha sido borrado correctamente. Si un sector no puede ser sobrescrito, se debe emitir una alerta para que el dispositivo sea sometido a un proceso de destrucción física.
- Reporte de Cumplimiento: Se debe generar un certificado de borrado seguro por cada dispositivo procesado, verificando que la eliminación de datos se realizó de acuerdo con los estándares establecidos.

#### ✓ Fabricantes y Soluciones

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- Blancco: Reconocido fabricante de software de borrado de datos con certificaciones a nivel global. Ofrecen soluciones para discos duros, SSDs, dispositivos móviles y entornos virtuales.
- Ontrack: Especializados en recuperación de datos, pero también ofrecen servicios de borrado seguro y destrucción física.
- Kroll Ontrack: Provee software para borrado de datos y destrucción física.
- Verbatim: Ofrece soluciones de software y equipos para borrado seguro de datos.

#### ✓ Alcance Técnico y Prerrequisitos

- Medios de Almacenamiento: El servicio debe abarcar diferentes tipos de medios de almacenamiento:
  - Discos Duros (HDD)
  - Unidades de Estado Sólido (SSD)

- o Dispositivos Móviles (smartphones, tabletas)
- o Cintas Magnéticas y Medios Ópticos
- **Prerrequisitos:** Los dispositivos deben estar en un estado funcional que permita la conexión al sistema de borrado. Los equipos con daño físico severo o sin posibilidad de encendido deben ser sometidos a la destrucción física como único método de borrado.
- **Logística Segura:** El proveedor debe garantizar la seguridad física de los dispositivos desde su recolección hasta su procesamiento final, utilizando vehículos y contenedores seguros.

✓ **Funcionamiento**

- **Recolección y Registro:** El proveedor recoge los dispositivos y los registra con su número de serie, marca, modelo y estado físico.
- **Borrado Lógico:** Los dispositivos funcionales se conectan al sistema de borrado seguro. El software aplica los algoritmos de sobrescritura para eliminar los datos de forma permanente.
- **Verificación:** Se realiza una validación sector por sector para confirmar que el borrado fue exitoso.
- **Destrucción Física:** Los dispositivos que fallan el borrado lógico o que están dañados son sometidos a un proceso de destrucción física, como la trituración o la desmagnetización.
- **Certificación:** Se emite un certificado por cada dispositivo, detallando el método de borrado y el cumplimiento de los estándares de seguridad.
- **Disposición Final:** Los restos de los dispositivos destruidos se disponen de manera ambientalmente responsable.

✓ **Elementos mínimos de la gestión del servicio**

El proveedor deberá ofrecer un servicio que incluya los siguientes componentes:

- **Hardware/Software** de última generación.
- **Licenciamiento:** Incluir todas las licencias necesarias para las funcionalidades requeridas.
- **Soporte y Mantenimiento:** Soporte técnico 24/7, parches de seguridad y actualizaciones de firmware.
- **Monitoreo y Gestión:** Herramientas de monitoreo centralizado y gestión remota para la administración del servicio.

### 3.8.2 SERVICIOS TECNOLÓGICOS PARA CIBERSEGURIDAD

Un servicio de ciberseguridad debe contemplar una arquitectura en capas, cubriendo la prevención, detección, respuesta y recuperación. Los elementos mínimos son:

- ▣ **ANÁLISIS DE VULNERABILIDADES:** el cual es un componente esencial de la estrategia de ciberseguridad de las compañías. Este servicio debe proporcionar una evaluación continua y exhaustiva de la seguridad de la infraestructura tecnológica, identificando, priorizando y reportando vulnerabilidades. El objetivo es mitigar los riesgos de manera proactiva, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

✓ **Funcionalidades**

El servicio debe incluir las siguientes funcionalidades clave:

- Escaneo de Vulnerabilidades: Realizar escaneos regulares y bajo demanda para identificar vulnerabilidades en la red, servidores, aplicaciones web, bases de datos y dispositivos de red.
- Gestión de Vulnerabilidades: Proporcionar una plataforma centralizada para el seguimiento, la priorización y la asignación de responsabilidades para la remediación de vulnerabilidades.
- Generación de Informes: Emitir informes detallados y ejecutivos, con análisis de tendencias, puntuaciones de riesgo y recomendaciones de mitigación. Los informes deben ser personalizados y adaptarse a las necesidades del negocio.
- Análisis de Cumplimiento: Verificar el cumplimiento con los estándares de seguridad y regulaciones (ej. ISO 27001, PCI DSS, NIST).
- Detección de Amenazas: Integrar bases de datos de amenazas actualizadas y técnicas de Inteligencia de Amenazas (Threat Intelligence) para identificar vulnerabilidades conocidas y exploits.
- API y Automatización: Facilitar la integración con otras herramientas de seguridad (ej. SIEM, SOAR) a través de APIs, permitiendo la automatización de flujos de trabajo de seguridad.

#### ✓ Fabricantes y Plataformas

El proveedor debe ser un aliado certificado de fabricantes en el mercado de ciberseguridad. Algunos de los fabricantes destacados en este campo son:

- Tenable: Reconocido por su plataforma Tenable.sc (Security Center) y Nessus Professional, ofrecen una amplia cobertura de vulnerabilidades y una gestión robusta.
- Qualys: Proporciona una suite integral en la nube para la gestión de vulnerabilidades, escaneo de aplicaciones web y cumplimiento.
- Rapid7: Ofrece la plataforma InsightVM, que combina el análisis de vulnerabilidades con la visibilidad de la exposición al riesgo en tiempo real.
- Otros fabricantes: Se pueden considerar proveedores que ofrezcan funcionalidades equivalentes y que cumplan con los estándares de seguridad de la industria.

#### ✓ Prerrequisitos y Alcances Técnicos

- Inventario de Activos: El interesado debe contar con acceso a un inventario completo y actualizado de los activos a escanear (direcciones IP, nombres de host, rangos de red, URLs de aplicaciones).
- Alcance del Servicio: El servicio debe ser aplicable a la infraestructura de red, servidores (Windows, Linux), dispositivos de red (switches, routers), bases de datos (SQL, Oracle), aplicaciones web (OWASP Top 10) y sistemas en la nube.
- Escaneo Interno y Externo: La solución debe ser capaz de realizar escaneos tanto desde el exterior (para identificar vulnerabilidades expuestas a internet) como desde el interior de la red (para detectar vulnerabilidades internas).
- Credenciales: Se debe contar con la capacidad de realizar escaneos autenticados (con credenciales de administrador o de usuario) para una detección más profunda y precisa.

### ✓ **Funcionamiento y Operación**

El servicio debe operar bajo un modelo gestionado, donde el proveedor es responsable de:

- Planificación y Programación: Acordar con el cliente la periodicidad de los escaneos (mensual, trimestral, etc.) y la ventana de mantenimiento para evitar impacto en la operación.
- Ejecución de Escaneos: Realizar los escaneos de manera programada o bajo demanda.
- Análisis y Priorización: Analizar los resultados del escaneo para priorizar las vulnerabilidades más críticas según el contexto del negocio.
- Entrega de Informes: Entregar informes técnicos y ejecutivos que incluyan la descripción de la vulnerabilidad, la severidad, las pruebas de explotación y las recomendaciones de mitigación.
- Seguimiento y Cierre: Colaborar con los equipos de TI del cliente en la remediación de las vulnerabilidades y verificar su corrección en escaneos posteriores.

☐ **ETHICAL HACKING:** es una evaluación de seguridad proactiva y controlada que simula un ataque de un hacker malicioso. Su objetivo es identificar y explotar vulnerabilidades en sistemas, redes y aplicaciones para que puedan ser corregidas antes de que sean explotadas por atacantes reales. Este servicio es un componente esencial de una estrategia de ciberseguridad integral, ya que evalúa la postura de seguridad de una organización desde la perspectiva del adversario.

### ✓ **Funcionalidades del Servicio**

Un servicio de hacking ético debe incluir las siguientes funcionalidades clave:

- Identificación de Vulnerabilidades: El equipo ético escanea y analiza sistemas, redes y aplicaciones para descubrir debilidades de seguridad.
- Explotación Controlada: Se intenta explotar las vulnerabilidades encontradas para demostrar el impacto potencial de un ataque.
- Análisis de la Postura de Seguridad: Evalúa la efectividad de los controles de seguridad existentes.
- Validación de Controles de Seguridad: Se verifica que las medidas de seguridad como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) estén configurados correctamente.
- Pruebas de Penetración de Aplicaciones Web: Se enfoca en identificar fallos en las aplicaciones web, como inyección SQL, scripting de sitios cruzados (XSS) y exposición de datos sensibles.
- Pruebas de Penetración de Redes (Internas y Externas): Evalúa la seguridad de la infraestructura de red para identificar puntos de entrada, como configuraciones erróneas de dispositivos, puertos abiertos o servicios vulnerables.
- Análisis de la Seguridad del Código: Revisa el código fuente de las aplicaciones para detectar vulnerabilidades antes de que se implementen.

### ✓ **Proveedores y Fabricantes**

Aunque el hacking ético es principalmente un servicio, a menudo se apoya en herramientas de software de fabricantes reconocidos. Se puede considerar la

colaboración con proveedores de servicios especializados en ciberseguridad que utilicen herramientas de los siguientes tipos de fabricantes:

- Fabricantes de Herramientas de Escaneo de Vulnerabilidades: Por ejemplo, Tenable (Nessus), Qualys y Rapid7. Estas herramientas automatizan el descubrimiento de vulnerabilidades conocidas.
- Plataformas de Prueba de Penetración: Metasploit es un ejemplo líder de una plataforma que facilita la explotación de vulnerabilidades.
- Proveedores de Servicios de Ciberseguridad Gestionados (MSSP): Empresas que ofrecen el servicio de hacking ético con equipos de expertos certificados.

### ✓ **Requisitos y Alcances Técnicos**

Para llevar a cabo un servicio de hacking ético de manera efectiva, se deben establecer los siguientes requisitos y alcances:

#### ● **Pre-requisitos:**

- c) Autorización formal: Se debe contar con una autorización por escrito de la gerencia para realizar las pruebas.
- d) Definición de Alcance: Se debe especificar claramente qué activos (direcciones IP, dominios, aplicaciones) están incluidos en la prueba y cuáles están excluidos.
- e) Plazos y horarios: Se deben acordar las fechas y horas para la ejecución de las pruebas.

#### ● **Alcances Técnicos:**

- o Pruebas de Caja Negra (Black-box): El equipo ético no tiene conocimiento previo de la infraestructura interna de la organización, simulando un ataque externo.
- o Pruebas de Caja Blanca (White-box): El equipo ético tiene acceso completo a la información de la red y el código fuente, simulando un ataque interno o un compromiso con privilegios.
- o Pruebas de Caja Gris (Gray-box): Se tiene un conocimiento parcial de la infraestructura, lo que simula un ataque de un usuario interno o con credenciales limitadas.

### ✓ **Funcionamiento y Seguridad**

El proceso del servicio de hacking ético se compone de varias fases, siempre bajo un estricto control y ética para garantizar la seguridad y disponibilidad de los sistemas:

- Recopilación de Información (Reconocimiento): Se busca información pública sobre la organización y sus sistemas.
- Escaneo de Puertos y Servicios: Se identifican los servicios y puertos abiertos en los activos definidos en el alcance.
- Análisis de Vulnerabilidades: Se utilizan herramientas automatizadas y análisis manual para encontrar vulnerabilidades.
- Explotación: Se intenta explotar las vulnerabilidades para demostrar el riesgo.
- Análisis Posterior y Reporting: Se elabora un informe detallado que documenta las vulnerabilidades encontradas, su impacto y las recomendaciones para su corrección.

Para que un servicio de ciberseguridad sea integral, este debe ser continuo y apoyarse en otras medidas como:

- Sistemas de Cifrado: Para proteger la confidencialidad de los datos.
- Gestión de Vulnerabilidades (Vulnerability Management): Un proceso continuo de identificación, evaluación y corrección de vulnerabilidades.
- Monitoreo y Detección (SOC): Un equipo de monitoreo de seguridad que utilice herramientas como SIEM (Security Information and Event Management) para detectar amenazas en tiempo real.
- Entrenamiento y Concienciación: Para educar a los empleados sobre las amenazas de seguridad y las mejores prácticas.

Un servicio de hacking ético no solo identifica fallas, sino que también ofrece un panorama completo de la postura de seguridad de la organización, permitiendo una toma de decisiones informada para mejorar las defensas.

- ❑ **ANÁLISIS FORENSE:** concebido como un componente esencial de una estrategia de ciberseguridad robusto. El objetivo es establecer un marco de repuesta ante incidentes que permita la recolección, preservación, análisis y presentación de evidencias electrónicas de manera forense, garantizando la integridad, autenticidad y cadena de custodia.

#### ✓ **Funcionalidades**

El servicio debe ser capaz de:

- Recopilación de Datos: Adquirir información de manera segura y forense de diversas fuentes, incluyendo, pero no limitado a, discos duros, memoria RAM, dispositivos móviles, y sistemas en la nube.
- Análisis de Malware: Identificar el tipo de malware, su comportamiento, origen y los activos afectados.
- Análisis de Tráfico de Red: Examinar registros de red y flujos de tráfico para detectar actividades sospechosas, movimientos laterales y exfiltración de datos.
- Recuperación de Datos: Restablecer datos eliminados o corruptos de dispositivos de almacenamiento.
- Análisis de Volcado de Memoria (Memory Dump Analysis): Examinar la memoria volátil del sistema para detectar procesos maliciosos, credenciales, y datos que no persisten en el disco.
- Generación de Informes: Proporcionar informes técnicos y ejecutivos detallados, documentando la metodología, el cronograma del incidente, el alcance del daño y las recomendaciones para la mitigación.

#### ✓ **Alcance Técnico y Prerrequisitos**

- El servicio debe ser aplicable a los siguientes entornos tecnológicos:
- Sistemas Operativos: Microsoft Windows, Linux (diversas distribuciones) y macOS.
- Dispositivos de Red: Routers, switches, firewalls, y otros dispositivos de gestión de red.
- Entornos Virtualizados: Soporte para plataformas como VMware, Hyper-V, y contenedores Docker.

- Infraestructura en la Nube: Compatibilidad con nubes públicas (AWS, Azure, GCP) y privadas.

#### ✓ **Prerrequisitos**

La compañía debe tener un equipo de respuesta a incidentes interno o un punto de contacto que colabore con el proveedor. Es crucial que se disponga de los permisos de acceso y las herramientas necesarias (como agentes de recolección de datos forenses) para permitir al proveedor operar de manera efectiva.

#### ✓ **Funcionamiento y Metodología**

El proceso de análisis forense debe seguir una metodología clara y documentada, que incluya las siguientes fases:

- Preparación: Acuerdos de servicio, comunicación y definición de roles y responsabilidades.
- Identificación: Detección del incidente de seguridad.
- Contención: Aislamiento de los sistemas afectados para prevenir la propagación del ataque.
- Erradicación: Remoción de los elementos maliciosos.
- Recuperación: Restauración de los sistemas a su estado normal.
- Análisis Forense: Recopilación de la evidencia, análisis detallado y documentación.
- Post-Incidente: Lecciones aprendidas y mejora de las políticas de seguridad.

#### ✓ **Fabricantes y Herramientas**

Se requerirá que el proveedor utilice herramientas y plataformas reconocidas en la industria para el análisis forense, que garantizan la integridad de la evidencia. Algunos de los fabricantes y herramientas aceptables incluyen:

- Magnet Forensics (Magnet AXIOM): Plataforma integral para el análisis de computadoras y dispositivos móviles.
- Cellebrite: Líder en análisis forense de dispositivos móviles.
- EnCase (OpenText): Una de las herramientas pioneras y más completas en forense digital.
- Volatile (Volatility Foundation): Herramienta de código abierto para el análisis de memoria.
- Wireshark: Herramienta de análisis de protocolos de red.

#### ✓ **Seguridad y Disponibilidad**

El servicio debe operar con los más altos estándares de seguridad y disponibilidad:

- Cadena de Custodia: Se debe garantizar una estricta cadena de custodia de la evidencia, documentando cada paso desde la recolección hasta el almacenamiento.
- Confidencialidad: Toda la información y los datos sensibles deben ser tratados con la máxima confidencialidad, con un acuerdo de no divulgación (NDA) firmado.
- Disponibilidad del Servicio: El proveedor debe ofrecer un servicio 24/7 para la respuesta a incidentes críticos, con tiempos de respuesta (SLA) definidos.

- **Confiability:** Las herramientas y métodos utilizados deben ser aceptables en un tribunal de justicia, lo que garantiza que las conclusiones puedan usarse en procedimientos legales si fuera necesario.
- Este servicio de análisis forense complementa la estrategia de ciberseguridad, permitiendo a la compañía no solo responder a los incidentes, sino también entender su naturaleza, mitigar el impacto y prevenir futuras vulneraciones.

☐ **INGENIERÍA SOCIAL:** la ciberseguridad no puede limitarse a la protección técnica de la infraestructura (firewall, antivirus, etc). El factor humano es una de las principales vulnerabilidades que los atacantes explotan para obtener acceso no autorizado. Un servicio de ingeniería social tiene como objetivo simular ataques controlados para evaluar la susceptibilidad del personal a la manipulación psicológica. Los resultados de esta evaluación permiten identificar y mitigar riesgos, fortalecer la cultura de seguridad y mejorar las capacidades de detección y respuesta de la organización. Un servicio integral de ciberseguridad debe ser seguro, confiable, disponible y esto no se puede lograr sin abordar las vulnerabilidades.

#### ✓ **Alcance Técnico del Servicio**

El servicio de ingeniería social deberá cubrir los siguientes escenarios de ataque, realizados de manera controlada y ética:

- **Ataques de Phishing:** Simulación de correos electrónicos maliciosos, con el objetivo de engañar a los empleados para que revelen información confidencial (credenciales de inicio de sesión, datos personales) o hagan clic en enlaces maliciosos. Se utilizarán técnicas avanzadas como el spear phishing (ataques dirigidos a individuos específicos) y el whaling (dirigidos a altos ejecutivos).
- **Ataques de Vishing (Voice Phishing):** Simulaciones de llamadas telefónicas fraudulentas para persuadir a los empleados a divulgar información sensible. Se imitarán escenarios comunes, como llamadas de soporte técnico o de la mesa de ayuda.
- **Ataques de Smishing (SMS Phishing):** Envío de mensajes de texto falsos para que los usuarios hagan clic en enlaces o descarguen aplicaciones maliciosas.
- **Ataques de Pretexting:** Creación de escenarios falsos (pretextos) para obtener información de los empleados. Por ejemplo, hacerse pasar por un proveedor o un compañero de trabajo que necesita información urgente.
- **Ingresos Físicos Controlados:** En algunos casos, se puede simular el acceso físico a las instalaciones para probar la efectividad de los controles de seguridad y la conciencia del personal ante la presencia de intrusos.

#### ✓ **Funcionalidades y Componentes del Servicio**

El servicio debe ser una solución completa que incluya las siguientes funcionalidades:

- **Planificación y Diseño de la Campaña:** El proveedor debe colaborar en la planificación de escenarios de ataque realistas y personalizados, adaptados al perfil de la organización.

- Ejecución de Ataques: El proveedor ejecutará los ataques de forma controlada, garantizando que no se cause daño a la infraestructura de la compañía.
- Plataforma de Monitoreo y Análisis: Se debe proveer una plataforma que permita monitorear la tasa de clics, la interacción con los mensajes y la recopilación de datos de la simulación.
- Informes y Recomendaciones: Al finalizar la campaña, el proveedor entregará un informe detallado que incluya los resultados, un análisis de las vulnerabilidades y recomendaciones específicas para mitigar los riesgos. El informe debe ser claro y conciso, con datos cuantitativos que demuestren el nivel de exposición de la organización.
- Capacitación y Concientización: El servicio debe incluir programas de capacitación y concientización para los empleados que hayan sido identificados como vulnerables.

#### ✓ **Requisitos Técnicos y Pre-requisitos**

- Dominio y Reputación de Correo Electrónico: Se deben utilizar dominios y direcciones de correo electrónico que simulen los de la compañía o sus proveedores de manera convincente.
- Plataforma Tecnológica: Se requiere una plataforma robusta que permita el despliegue masivo de correos electrónicos, llamadas telefónicas y mensajes de texto, sin afectar la operación diaria.
- Personal Calificado: El proveedor debe contar con personal especializado en ciberseguridad, con certificaciones relevantes en el campo de la ingeniería social y las pruebas de penetración.
- Legalidad y Ética: El servicio debe estar sujeto a un acuerdo contractual que establezca claramente los alcances y límites del mismo, garantizando el cumplimiento de la normativa de protección de datos y el respeto a la privacidad del personal.

#### ✓ **Fabricantes y Proveedores (Ejemplos)**

Existen múltiples proveedores especializados en servicios de ingeniería social. Algunos de los más reconocidos incluyen:

- KnowBe4: Ofrece una plataforma integral para la gestión de la concientización en seguridad, con simulaciones de phishing automatizadas y programas de capacitación.
- Cofense: Es un líder en la lucha contra el phishing, con soluciones para la simulación de ataques y el entrenamiento del personal.
- Terranova Security: Ofrece una amplia gama de herramientas y cursos para concientizar sobre el phishing y la ingeniería social.

#### ✓ **Funcionamiento del Servicio (Ciclo Operacional)**

- Planificación y Alcance: Definición de los objetivos, el público objetivo y los vectores de ataque.
- Preparación de la Campaña: Creación de los escenarios de ataque (correos electrónicos, mensajes, páginas web falsas).
- Ejecución de la Campaña: Lanzamiento de los ataques en un entorno controlado y monitoreado.

- Recolección de Datos: Recopilación de métricas clave, como el número de clics en enlaces maliciosos, la tasa de apertura de correos electrónicos y la información entregada por los usuarios.
- Análisis y Reporte: Evaluación de los resultados y preparación de un informe detallado con hallazgos y recomendaciones.
- Capacitación y Refuerzo: Implementación de programas de capacitación para fortalecer las defensas humanas.

### 3.8.3 SERVICIOS ESPECIALIZADOS PARA CIBERSEGURIDAD

ETB, en su rol de integrador estratégico de soluciones, tecnologías y servicios, tiene como prioridad fortalecer de manera continua sus capacidades de gestión, atención y respuesta. El objetivo es enfrentar de forma proactiva y efectiva los desafíos que las amenazas digitales imponen a diario, asegurando así la integridad y la continuidad de sus operaciones y la de sus clientes. Este enfoque proactivo permite a la empresa no solo reaccionar, sino también anticiparse a los riesgos, consolidando su posición como un socio confiable en el ecosistema digital.

El servicio para contratar será de extremo a extremo y estará diseñado para proveer y gestionar soluciones de ciberseguridad que protejan la infraestructura de la organización en sus diferentes capas, asegurando la continuidad del negocio y el cumplimiento normativo.

#### xxiv. Capacidades de los servicios especializados por solución

- Inteligencia y Cacería de Amenazas (Threat Intelligence & Hunting): Habilidad para realizar cacería de amenazas de forma proactiva, identificar IOCs y TTPs, y contextualizar la inteligencia de amenazas para la toma de decisiones.
- Gestión de Vulnerabilidades y Análisis de Riesgos: Destreza para gestionar el ciclo de vida de las vulnerabilidades, desde su detección y clasificación hasta la priorización de su remediación, utilizando plataformas de escaneo y gestión de riesgos.
- Seguridad de Correo y Antispam: Experiencia en la implementación y gestión de soluciones de seguridad de correo, incluyendo la protección contra amenazas avanzadas como phishing, malware y spam.
- Protección Web, WAF y Proxy: Capacidad para configurar y administrar servicios de protección web, incluyendo la implementación de firewalls de aplicaciones web (WAF) para defenderse de ataques comunes como la inyección SQL y el cross-site scripting (XSS).
- Pruebas de Ethical Hacking e Ingeniería Social: Destreza para simular ciberataques de manera controlada y ética, identificar vulnerabilidades en la infraestructura, aplicaciones y la "capa humana", y proporcionar informes detallados para mitigar los hallazgos.
- Monitoreo de Marca y Detección de Fugas de Datos (DLP): Conocimiento para monitorear el uso de la marca corporativa en internet, detectar fraudes y suplantaciones de identidad, así como identificar y prevenir la fuga de datos sensibles.
- Análisis Forense y Detección y Respuesta en Endpoints (EDR): Habilidad para realizar análisis forense en sistemas comprometidos para determinar la causa raíz,

el alcance del incidente y la información afectada. Esto incluye la gestión de plataformas de EDR y la investigación de amenazas.

- Seguridad de Aplicaciones (SAST, DAST, SCA) y Desarrollo Seguro: Capacidad para integrar la seguridad en el ciclo de desarrollo de software (DevSecOps), utilizando herramientas de análisis estático (SAST), dinámico (DAST) y de composición de software (SCA) para identificar vulnerabilidades.
- Seguridad en la Nube (Cloud & CASB): Expertise en la evaluación y gestión de la postura de seguridad en entornos de nube pública e híbrida. Esto incluye la implementación y operación de intermediarios de seguridad de acceso a la nube (CASB) para proteger datos en entornos SaaS.
- Operaciones de Seguridad (SecOps) y SOAR: Habilidad para gestionar las operaciones de un centro de operaciones de seguridad (SOC), incluyendo la correlación y análisis de eventos (SIEM), y la automatización de la respuesta a incidentes a través de plataformas SOAR.
- Protección de Identidades (IAM, PAM) y NAC: Dominio en la gestión de identidades y accesos (IAM), incluyendo la administración de accesos privilegiados (PAM) y el control de acceso a la red (NAC) para asegurar que solo los usuarios y dispositivos autorizados accedan a los recursos.
- Protección de OT/IoT: Capacidad para identificar, monitorear y proteger sistemas de tecnología operativa (OT) e internet de las cosas (IoT) de ciberataques, asegurando la continuidad de la producción.

▣ **CISO como servicio:** En el panorama actual de amenazas digitales en constante evolución, la ciberseguridad ya no es un simple requerimiento técnico, sino un pilar estratégico para la supervivencia y el crecimiento de cualquier organización. La implementación de un Chief Information Security Officer (CISO) as a Service (CISOaaS) se presenta como una solución integral y costo-efectiva. Este servicio externalizado provee la experiencia, la dirección estratégica y la supervisión necesarias para establecer, mantener y madurar un programa de ciberseguridad robusto sin la necesidad de contratar a un ejecutivo a tiempo completo.

#### ✓ **Alcance**

El rol del CISOaaS va más allá de la gestión técnica y abarca un espectro completo de responsabilidades, sus actividades principales incluyen:

- Liderazgo Estratégico: Desarrollar e implementar la estrategia de ciberseguridad alineada con los objetivos de negocio. Esto incluye la definición de la visión, misión y los objetivos a largo plazo en materia de seguridad de la información.
- Gestión de Riesgos: Identificar, evaluar, mitigar y monitorear los riesgos de seguridad de la información. El CISO creará un marco de gestión de riesgos que incluirá la identificación de activos críticos, el análisis de vulnerabilidades y la priorización de controles.
- Gestión de Políticas y Estándares: Crear, revisar y comunicar las políticas de seguridad de la información (por ejemplo, política de uso aceptable, política de control de acceso, etc.) y asegurar que la organización cumpla con los estándares y marcos regulatorios relevantes (como ISO 27001, NIST, GDPR, etc.).
- Respuesta a Incidentes: Establecer un plan de respuesta a incidentes de seguridad (IRP) que permita a la organización reaccionar de manera

efectiva, minimizar el impacto de las brechas de seguridad y recuperarse rápidamente.

- Concientización y Capacitación: Diseñar e implementar un programa de concientización y formación en ciberseguridad para todo el personal, fortaleciendo la cultura de seguridad.
- Gestión de la Continuidad del Negocio (BCM): Asegurar la integración de la seguridad de la información en el plan de continuidad del negocio y el plan de recuperación ante desastres (DRP) para garantizar la resiliencia operativa.

#### ✓ Modelos de Gestión y Auditoría

El servicio de CISOaaS debe basarse en un modelo de gestión y auditoría estructurado para asegurar la mejora continua.

- Modelo de Gestión: Se propone un modelo basado en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), un principio fundamental de la norma ISO 27001.
  - Planificar (Plan): Establecer los objetivos y procesos necesarios para la gestión de la seguridad.
  - Hacer (Do): Implementar y operar los controles definidos.
  - Verificar (Check): Medir el desempeño a través de indicadores clave de rendimiento (KPIs) y métricas, y auditar el sistema.
  - Actuar (Act): Tomar acciones correctivas y de mejora para el sistema.
- Auditoría y Monitoreo: El CISO realizará auditorías internas periódicas para verificar la efectividad de los controles de seguridad. También facilitará auditorías externas y pruebas de penetración (pentesting) para validar la postura de seguridad de la organización desde una perspectiva independiente.

#### ✓ Componentes Técnicos y de Funcionamiento para un Servicio Integral

Para que el servicio sea verdaderamente integral, el CISOaaS debe coordinar y supervisar los siguientes componentes técnicos:

- Sistema de Gestión de Seguridad de la Información (SGSI): El CISO es el principal responsable de la implementación y mantenimiento del SGSI, garantizando que el alcance, las políticas y los controles cubran toda la organización. Este sistema proporciona un marco formal para la gestión de riesgos de seguridad de la información.
- Gestión de la Identidad y el Acceso (IAM): Supervisar la implementación de soluciones de IAM para controlar quién tiene acceso a qué recursos, incluyendo el uso de la autenticación multifactor (MFA) y el principio del mínimo privilegio.
- Defensa en Profundidad: Asegurar la implementación de múltiples capas de seguridad, incluyendo firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), protección de endpoints (EDR/XDR) y filtros de correo electrónico.
- Monitoreo y Detección: Establecer un Centro de Operaciones de Seguridad (SOC) o un servicio de Monitoreo 24/7 para detectar actividades anómalas en tiempo real. Esto incluye la gestión de eventos e información de seguridad (SIEM).

- Seguridad de la Red y la Nube: Gestionar la seguridad de la infraestructura de red, tanto on-premise como en la nube, incluyendo la configuración de seguridad, la segmentación de red y la gestión de vulnerabilidades.
  - Gestión de la Continuidad del Negocio (BCM) y Recuperación ante Desastres (DR): El CISO se asegura de que existan planes documentados y probados para recuperar las operaciones críticas del negocio después de un incidente grave. Esto incluye la definición de Objetivos de Tiempo de Recuperación (RTO) y Objetivos de Puntos de Recuperación (RPO).
- ☐ **Gestión remota SOC:** Los servicios de ciberseguridad descritos anteriormente podrán ser provistos de forma remota, 24x7x365, desde un Centro de Operaciones de Seguridad (SOC) del interesado. Este SOC debe ser un entorno centralizado y seguro, diseñado para el monitoreo, detección, análisis, contención y respuesta a incidentes de seguridad en tiempo real.
- **Monitoreo Continuo:** El equipo del SOC debe ser capaz de monitorear la infraestructura del cliente las 24 horas del día para detectar actividades anómalas y amenazas en tiempo real.
  - **Gestión y Soporte:** Las operaciones, la administración y el soporte de las diferentes herramientas de ciberseguridad se realizan de forma remota, a través de conexiones seguras y con el uso de plataformas centralizadas.
  - **Certificaciones del Personal:** El equipo del SOC debe contar con certificaciones profesionales que validen su experticia. Se valoran certificaciones de seguridad de fabricantes como Fortinet, Palo Alto Networks, Check Point, Cisco, Microsoft y otras, así como certificaciones de la industria reconocidas globalmente, tales como:
    - **GIAC (Global Information Assurance Certification):** Certificaciones especializadas en diversas áreas de la seguridad.
    - **CISSP (Certified Information Systems Security Professional):** Certificación de seguridad de la información de alto nivel.
    - **CEH (Certified Ethical Hacker):** Para roles de hacking ético y análisis de vulnerabilidades.
    - **CCSP (Certified Cloud Security Professional):** Para la seguridad en la nube.
    - **CompTIA Security+:** Para roles de seguridad de nivel de entrada.
- ☐ **Requisitos mínimos de los servicios especializados del interesado:** Los servicios especializados deberán contar con las herramientas, tecnologías y capacidades para garantizar la óptima prestación de los servicios de ciberseguridad, por tanto, ETB presenta el alcance de los servicios especializados como parte integral del servicio.
- l. **Expertos en Soporte y Migración:** Profesionales enfocados en la planificación, ejecución y soporte técnico de la migración de las diferentes herramientas de ciberseguridad. Sus funciones incluyen la preparación de la infraestructura, la configuración inicial y el acompañamiento durante el proceso de transición.
- m. **Expertos en Herramientas de Ciberseguridad (Senior / Junior):** Personal con experiencia en la operación, configuración y administración de herramientas de seguridad. El nivel **Senior** se encarga de la gestión de soluciones complejas como

SIEM y WAF, mientras que el nivel **Junior** brinda apoyo en tareas de soporte y configuración básica.

- n. **Expertos en Análisis de Vulnerabilidades y Código de Aplicaciones:** Especialistas en la ejecución de análisis estáticos y dinámicos para identificar vulnerabilidades en aplicaciones y sistemas. El nivel **Senior** lidera las auditorías y gestiona la remediación, mientras que el **Junior** se enfoca en la ejecución de las pruebas.
- o. **Expertos en Análisis Forense (Senior / Máster):** Responsable de la recolección de evidencia digital, el análisis de datos volátiles y no volátiles, y la elaboración de informes periciales. El nivel **Máster** también se encarga de la coordinación de equipos y el desarrollo de metodologías.
- p. **Expertos en Auditoría (Senior / Máster):** Encargado de evaluar la postura de seguridad de la organización, auditar políticas y verificar el cumplimiento normativo. El nivel **Máster** lidera auditorías complejas y asesora a la alta dirección.
- q. **Expertos en Ethical Hacking (Senior / Máster):** Profesionales con habilidades avanzadas en la simulación de ataques para identificar vulnerabilidades. El nivel **Máster** está a cargo de las pruebas más complejas, como las de caja negra, y la creación de exploits personalizados.
- r. **Expertos en Ingeniería Social (Senior / Máster):** Especialistas en el diseño y ejecución de campañas de ingeniería social para evaluar la conciencia de seguridad de los empleados. Un **Máster** en este rol diseña programas de entrenamiento y sensibilización a medida.
- s. **Expertos en SGSI / MSPI (Senior / Máster):** Lideran la implementación, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI). Un **Máster** es responsable de la estrategia de seguridad y la gestión de riesgos a nivel corporativo.

- ▣ **Servicio integral de soporte para migración de herramientas de ciberseguridad** El servicio de soporte para migración de herramientas de ciberseguridad se enfoca en facilitar una transición fluida y segura de las soluciones de seguridad existentes a nuevas plataformas. Este proceso abarca desde una evaluación inicial del entorno actual para comprender la configuración y dependencias, hasta la planificación detallada del proyecto que minimice el impacto en las operaciones diarias. El alcance incluye la ejecución técnica de la migración, asegurando que los datos de configuración, políticas de seguridad y registros históricos sean transferidos de manera precisa e íntegra. Además, se proporciona validación post-migración para confirmar que todas las funcionalidades operan correctamente, y se ofrece capacitación al personal técnico para que pueda gestionar la nueva herramienta de manera eficiente. Este enfoque integral no solo reduce los riesgos asociados a la migración, sino que también garantiza la continuidad de la protección y maximiza el retorno de la inversión en la nueva tecnología.

### 3.8.4 ENTREGABLES

Dentro del proceso de presentación de oferta para el presente RFP, se requiere que el OFERENTE suministre los siguientes documentos:

- Certificación de partner del fabricante o fabricantes que soportan su oferta, debe evidenciarse el nivel de partner, dicha certificación deberá tener una vigencia inferior o igual a 30 días calendario.

Se debe especificar como parte de la respuesta punto a punto el nombre del fabricante con el cual están presentando oferta por cada uno de los componentes de servicio.

### 3.8.5 SERVICIOS DE OPERACIÓN, GESTIÓN Y ASEGURAMIENTO

La prestación del servicio integral de administración, operación, soporte y mantenimiento de los servicios y/o productos ofertados, EL OFERENTE deberá realizar la gerencia del proyecto con metodología PMP para la implementación y la prestación de los servicios de TI con base en el marco de referencia de ITIL para la operación, gestión y aseguramiento del servicio. Esta gestión debe ser liderada por el gerente de servicio o responsable que disponga el OFERENTE garantizando que tanto las actividades de planeación, operación, seguimiento, mejoramiento continuo y documentación adelantadas por el equipo de trabajo del proyecto se realicen con criterios de eficiencia y eficacia.

En el marco del contrato se contempla, entre otras, la responsabilidad de canalizar todos los incidentes y requerimientos de soporte técnico de los clientes ETB y garantizar los recursos y procedimientos de atención y seguimiento necesarios para brindar la solución definitiva de la totalidad de tales solicitudes; estableciendo un único centro de contacto (comunicación telefónica, correo electrónico y vía internet) para la atención de las necesidades de los clientes ETB en cuanto a la recepción, registro, análisis, solución, escalamiento, seguimiento y cierre de todas las solicitudes en el software de gestión de servicios provisto por EL OFERENTE.

El oferente deberá adelantar la gestión de incidentes y requerimientos, el cual permite:

- Registrar, atender, gestionar y escalar las solicitudes reportadas.
- Medir, auditar y generar todos los reportes estadísticos relacionados con la naturaleza de los servicios ofrecidos y solicitados
- Parametrizar los indicadores de cumplimiento de los niveles de servicio requeridos.

El OFERENTE debe contar con expertos en temas de fortalecimiento de infraestructura tecnológica y con el equipo de especialistas proponer iniciativas y/o acompañar y apoyar aquellas que durante el desarrollo del contrato se emprendan, de tal forma que contribuya ampliamente a que la infraestructura tecnológica sea adecuada para obtener información consistente y confiable y le permita a la entidad realizar una buena gestión y seguimiento de los proyectos que realiza para cumplir su misión y tomar decisiones apropiadas de una manera efectiva.

EL OFERENTE como parte de sus servicios de administración y gestión de plataformas e infraestructura, deberá cumplir como mínimo con las actividades listadas a continuación.

- Administración y soporte de la infraestructura administrada.

- Instalación y configuración de los sistemas operativos /IOS para la infraestructura administrada.
- Definir, revisar y mantener las políticas de back up y restore de los servicios y/o productos gestionados.
- Gestión de usuarios, administración y mantenimiento de los usuarios definidos en el sistema (altas, bajas, control de permisos y accesos).
- Gestión de incidencias de los sistemas.
- Investigación, diagnóstico y solución de problemas de la infraestructura administrada.
- Aplicación y actualización de “fixes” sobre el software de la infraestructura administrada.
- Monitoreo y revisión de LOGS de forma proactiva sobre la infraestructura administrada.
- Configuración y monitoreo del entorno de red para los servicios de networking, seguridad o nube pública a administrar.
- Recopilación y análisis de estadísticas para mejorar el rendimiento del sistema.
- Definición y mantenimiento de la configuración de alarmas definidas en las herramientas de gestión y monitoreo que disponga ETB para la infraestructura administrada.
- Entonación y afinamiento (Tunning) de la infraestructura administrada.
- Realización de tareas de “Hardening” para los sistemas operativos de los servicios de nube administrados.
- Realización de actividades necesarias sobre la infraestructura para cumplir con las políticas de seguridad de la información establecidas por ETB.
- Elaborar y actualizar cronogramas de mantenimiento que permitan mantener la infraestructura física en condiciones adecuadas y los componentes de software actualizados y protegidos.
- Escalar a los fabricantes de hardware y software los caso que se requieran para mantener actualizada y funcionando la infraestructura administrada.
- Hacer seguimiento de los casos escalados a los fabricantes de hardware y software y mantenerlos actualizados en las herramientas que ETB ha dispuesto para ello.
- Identificar los riesgos sobre la infraestructura administrada, definir y ejecutar los respectivos planes de mitigación.
- Realizar las configuraciones necesarias para el monitoreo y gestión de los diferentes componentes de la infraestructura administrada.
- Proponer, recomendar e implementar políticas de gestión sobre la infraestructura administrada.
- Participar en la ejecución de ventanas programadas con los clientes

### 3.8.5 FINALIZACIÓN

#### Empalme de implementación

Al cierre de la implementación del contrato, el proveedor deberá hacer entrega de la documentación, en formato genérico, correspondiente a transferencia de conocimiento en cuanto a:

- Funciones de configuración y operación.

- Metodología de aplicación de los procesos y conocimientos ejecutados durante el periodo de implementación.
- Documentación e información adicional asociada a la fase de implementación solicitada por el supervisor de contrato de ETB.

ETB verificará la información suministrada y verificará igualmente la correcta aplicación de los procesos documentados; así mismo, solicitará visitas de campo (si aplica) de acuerdo con las actividades allí descritas.

#### □ **Empalme en Operación**

Durante la operación del contrato, el proveedor deberá hacer la actualización a la documentación de transferencia de conocimiento, si ha existido algún cambio, frente a la documentación entregada en la fase de implementación incluyendo la documentación e información adicional asociada a la fase de operación solicitada por el supervisor de contrato de ETB.

#### □ **Empalme de salida**

El oferente deberá contemplar y realizar el empalme previo a la finalización del contrato, entendido como la entrega final de las actividades ejecutadas y transferencia de conocimiento al personal que sea designado por ETB.

De acuerdo con lo anterior, el proveedor con quien llegue a suscribirse el contrato producto de esta oferta; sin costo adicional para ETB, deberá garantizar el periodo de empalme final, bajo las siguientes consideraciones:

- Fecha de realización: Previo a la finalización del contrato.
- Duración: 15 días
- Tipo de empalme: Presencial.
- Metodología:
  - o Funciones de configuración y operación.
  - o Entrega y revisión de la documentación en formato genérico.
  - o Metodología de aplicación de los procesos y conocimientos ejecutados durante el periodo de implementación.
  - o Documentación e información adicional asociada a la fase de implementación solicitada por el supervisor de contrato de ETB.

NOTA: Al finalizar el periodo de empalme de salida, se suscribirá un acta en la que conste que se desarrolló de manera efectiva dicho proceso y esta acta será insumo para el pago de la última factura del contrato.

### **3.8.5 PROCEDIMIENTO PARA INCORPORAR NUEVOS ÍTEMS**

ETB revisará que los nuevos ítems se enmarquen en el objeto del contrato y, particularmente en cada línea de negocio, solicitará oferta a todos los Aliados habilitados, la cual debe ser presentada en la herramienta dispuesta por ETB y dentro de la hora señalada y con precios soportados y razonables de acuerdo con el mercado. Posteriormente, los nuevos ítems serán incluidos al Acuerdo Marco mediante acuerdo suscrito por Las Partes.

### **FIN DE LOS TÉRMINOS DE REFERENCIA BORRADOR**

**Canales de radicación oficial:**

**Físico:** Carrera 8 No 20 - 56 Piso 1 Ventanilla de Correspondencia

**Digital:** [gestioncorrespondencia@etb.com.co](mailto:gestioncorrespondencia@etb.com.co)



07-07.7-F-025-v.7

01/08/2025

*"Una vez impreso este documento, se considerará **documento no controlado**".*