ÁREA SOLICITANTE:	OFICINA ASESORA DE PLANEACION
RESPONSABLE:	PROFESIONAL UNIVERSITARIO SISTEMAS DE INFORMACIÓN
FECHA DE ELABORACIÓN:	19 DE OCTUBRE DE 2022
FUNDAMENTO TÉCNICO LEGAL:	LEY 142 DEL 1994 Por la cual se establece el régimen de los servicios públicos domiciliarios y se dictan otras disposiciones. LEY 80 DE 1993 - principios de la contratación pública LEY 1712 DE 2014 - Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. ACUERDO No. 005-2022 Manual de contratación Empresa de Servicios Públicos de Chía Emserchia E.S.P.
ASUNTO:	SUMINISTRO DE LA SUSCRIPCION A LA HERRAMIENTA HARMONY EMAIL CON EL FIN DE PROTEGER LOS CORREOS ELECTRONICOS CONTRA PHISHING Y MALWARE PARA LA EMPRESA DE SERVICIOS PUBLICOS DE CHIA EMSERCHIA E.S.P

DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER

Actualmente la empresa de servicios públicos de Chía Emserchia ESP presta sus servicios de acueducto, alcantarillado, aseo y complementarios a más de 45.000 usuarios. Emserchia ESP cuenta actualmente con el servicio de correo en la nube Google Workspace y los usuarios de Emserchia ESP se mantienen comunicados fácilmente por medio del correo electrónico y por lo tanto es indispensable para brindar una comunicación rápida y eficiente dentro y fuera de nuestra empresa logrando reducción de costos y simplificando procesos.

La seguridad proporcionada por Google no es suficiente ante los diferentes riesgos que se han venido incrementando durante los últimos años , cuyas estadísticas muestran que mas del 90% de los ataques contra organizaciones parten de un correo electrónico malicioso y el 75% de los ataques de Rasomware se trasmiten por correo electrónico como:

- Ataques sofisticados de phishing
- Ataques de malware que afectan la productividad
- Ataques de adquisision de cuentas, robo de credenciales
- Fuga de datos a travez del correo

Por esta razón se hace necesario adquirir un servicio de protección, especializado, contra amenazas trasmitidas por correo electrónico.
La solución debe deberá proporcionar un servicio para 100 (cien) usuarios para seguridad de correo electrónico en la Nube vía API, por un año.

Servicio en la nube de fabricante, (SaaS), sin necesidad de un proxy, dispositivo o agente en el punto final. Implementación escalable y rápida que utilice configuraciones de políticas listas para usar y flujos de trabajo de remediación.

La solución debe proveer protección contra los siguientes Ciber ataques:

- Prevención Ataques a Correo electrónico, como Phishing, Spoofing, Spam
- Detección de Malware o archivos maliciosos (archivos adjuntos en correos, archivos subidos a aplicaciones de colaboración y compartición)
- Anomalías de usuarios y Uso no autorizado de inicios de sesión (Indicios de robo de cuenta).

Uso no autorizado de aplicaciones SaaS también conocido como Shadow IT.

La solución debe permitir gestionar la detección, investigación y reparación de amenazas desde un panel de gestión de amenazas unificado.

La solución debe realizar un escaneo histórico del contenido de los correos de al menos 14 días atrás desde que la herramienta se active.

La solución debe utilizar protocolos de cifrado modernos para salvaguardar la organización.

La solución debe ser escalable y nativa de nube para soportar crecimiento a cientos de miles de usuarios.

La solución debe permitir que la entidad pueda extender el servicio, en un futuro, a defensas contra Ciber Amenazas, en las siguientes aplicaciones SaaS de colaboración y compartición de archivos:

- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft Teams
- Google Drive
- Box
- Dropbox
- Citrix ShareFiles
  Slack

La solución debe bloquear sofisticados ataques de ingeniería social, como la suplantación de identidad, phishing de día cero y Business Email Compromise (BEC) usando motores de Inteligencia Artificial

La solución debe inspeccionar los metadatos, archivos adjuntos, enlaces e idioma de la comunicación, así como todas comunicaciones históricas, para determinar relaciones de confianza previas entre el emisor y el receptor del correo para identificar la suplantación de identidad del usuario o de los mensajes fraudulentos.
La solución debe proteger los correos electrónicos de entrada, salientes y la comunicación interna en tiempo real para prevenir ataques laterales y amenazas internas.

La solución debe proveer prevención en línea es decir intercepción de correo antes que llegue al usuario final. Bloqueando los correos electrónicos maliciosos antes de que lleguen a la bandeja de entrada.

La solución debe realizar la verificación de cientos de indicadores de ataque sobre el correo electrónico como la verificación DMARC ,SPF o DKIM para verificar que un correo electrónico se origina en el supuesto dominio de origen.

La solución debe tener modos de detección seguidos de métodos de remediación de ciberataques realizando análisis fuera de línea.

La solución no debe requerir cambios en los registros MX de DNS, y ser invisible para los atacantes y a través de inteligencia artificial evitar ataques evasivos y sofisticados.

La solución debe detectar cuando los piratas informáticos utilizan el dominio de una empresa para hacerse pasar por la marca o sus empleados.

La solución debe escanear el documento HTML y generar un nuevo archivo solo con las etiquetas designadas como "seguras"; y deseado.

La solución reconocerá los correos electrónicos de phishing basados en la reputación de la URL a través de una base de datos de inteligencia en la nube.

La solución debe detectar y prevenir de los enlaces y URL maliciosos dentro del asunto, el cuerpo de los correos electrónicos, analizando en detalle todas las partes del url. para asegurarse de que no instalen malware o apunten a un dominio comprometido.

La solución debe analizar y abrir enlaces URL y reescribir el enlace para que los usuarios finales sepan que la solución escaneó el destino.
La solución debe ser capaz de poner en cuarentena correos maliciosos y debe proveer al usuario opciones para recuperarlos.

La solución debe contar con motores de seguridad para protección contra spam y capacidades aprendizaje automático y de acciones automatizadas como marcar como Spam, moverlo a la carpeta Spam/Junk.y cuarentena.

La solución debe tener un periodo de retención de correos electrónicos originales en cuarentena de al menos 180 días.

La solución debe tener un periodo de retención de los metadatos de los correos electrónicos analizados maliciosos por al menos 180 días

La solución debe tener la capacidad de remediar las amenazas que llegan a las bandejas de entrada de los usuarios, desde la interface de gestión debe poder realizar la identificación, análisis y corrección. Si llega un correo electrónico o un archivo, que se puedan tomar medidas inmediatas en miles de bandejas de entrada con unos pocos clics, sin PowerShell ni codificación de ningún tipo.

La solución debe incluir capacidades de "Sandboxing" resistente a la evasión para bloquear el malware de día cero, con un análisis dinámico en un entorno virtual aislado y escalable basado en la nube.

La solución debe admitir capacidades CDR *Content disarm and Reconstruction es decir, podrá limpiar los documentos o imágenes adjuntos en los correos electrónicos de contenido malicioso.
La solución debe tener protección antivirus/malware basada en firmas.

Escanear todos los archivos intercambiados interna y externamente en busca de enlaces maliciosos, códigos u otros componentes de ataques avanzados.

La solución debe detectar directamente el comportamiento malicioso y poner en cuarentena los archivos antes de que la amenaza se propague.

La solución debe contar con un motor que analice el comportamiento utilizando un algoritmo de aprendizaje automático que crea un perfil basado en información histórica de eventos, incluidas las ubicaciones y horas de inicio de sesión, el comportamiento de transferencia de datos y los patrones de mensajes de correo electrónico.

La solución debe detectar y alertar de anomalías de comportamiento de usuarios, como inicios de sesión sospechosos (por ejemplo, visto en dos diferentes ubicaciones, mala reputación de IP) , acciones sobre el correo inusuales , como reseteo de password anormales, o renvió de correos a direcciones externas, envío correos electrónicos a una velocidad que es inusual para su comportamiento anterior.

La solución debe evitar ataques avanzados de apropiación de cuentas aumentando los procesos de autenticación, evitar usuarios no autorizados y los dispositivos comprometidos accedan a su correo electrónico en la nube o a las aplicaciones SaaS.

La solución detectará y proporcionará informes de aplicaciones de Shadow IT y top de usuarios.

La solución debe proporcionar un informe de evaluación de riesgos de la aplicación.

Debe mantener logs de cada evento y comunicación para garantizar cumplimientos normativos.

Proveer tableros (Dashboards) detallados de los problemas de seguridad con el uso de las aplicaciones.

Registrando la cantidad usuarios, archivos, recursos compartidos, enlaces, inicios de sesión, y detecciones de amenazas.

Así las cosas, es necesario realizar la contratación del suministro de la herramienta HARMONY EMAIL DE CHECK POINT, PARA LA protección, especializada, contra amenazas trasmitidas por correo electrónico.

POBLACIÓN BENEFICIADA	POBLACIÓN INTERNA Se beneficiarán: Se benefician todos los funcionarios dela entidad al contar con la herramienta HARMONY EMAIL para protegernos de ataques de los ciberdelincuentes y evitar injeccion de código malicioso en el dominio de correo de Emserchia ESP. POBLACIÓN EXTERNA Se beneficiarán: Todos los usuarios de Emserchia E.S.P. ya que con la herramienta HARMONY EMAIL evitaremos que se propague algún correo malicioso y pueda afectar los usuarios externos a nuestra Entidad.
VIABILIDAD DEL PROYECTO Y SU IMPACTO SOCIAL, ECONÓMICO Y AMBIENTAL	Los ataques cibernéticos contra las Organizaciones han venido incrementándose durante los últimos años, y la gran mayoría parten de un correo electrónico malicioso llegando a inyectar malware como Rasonware, phishing, malware de dia cero, robo de credenciales, fuga de datos que afectan la productividad de nuestra Empresa. Por esta razón se hace necesario adquirir un servicio de protección, especializado, contra amenazas trasmitidas por correo electrónico.

DESCRIPCIÓN DEL OBJETO A CONTRATAR			
NATURALEZA DEL OBJETO	BIENES ☐	SERVICIOS ☒	OBRA PÚBLICA ☐
	CONSULTORÍA ☐	INTERVENTORÍA ☐	
	OTROS ☐	¿CUAL?:	

RUBRO POR AFECTAR	FUNCIONAMIENTO ☒	INVERSIÓN ☐

OBJETO

SUMINISTRO DE LA SUSCRIPCION A LA HERRAMIENTA HARMONY EMAIL CON EL FIN DE PROTEGER LOS CORREOS ELECTRONICOS CONTRA PHISHING Y MALWARE PARA LA EMPRESA DE SERVICIOS PUBLICOS DE CHIA EMSERCHIA E.S.P

VALOR:

DIECISIETE MILLONES CUATROSCIENTOS SESENTA MIL PESOS MCTE ($17.460.000) INCLUIDO IMPUESTOS QUE LE SEAN APLICABLES.

FORMA DE PAGO

LA EMPRESA CANCELARÁ AL CONTRATISTA EL VALOR DEL CONTRATO DE LA SIGUIENTE MANERA: UNICO PAGO PREVIA GENERACION DE FACTURA ELECTRONICA INCLUIDO IMPUESTOS QUE LE SEAN APLICABLES Y CON COPIA DE LOS PAGOS DE PARAFISCALES DE CONFORMIDAD CON EL ARTÍCULO 9 DE LA LEY 828 DE 2003 Y EL ARTÍCULO 23 DE LA LEY 1150 DE 2007.

PLAZO

El plazo para la ejecución del presente contrato será de un (1) mes contados a partir del perfeccionamiento del contrato y acta de inicio.

LUGAR DE EJECUCIÓN

La entrega de los equipos y/o prestación del servicio se realizará en el municipio de Chía, Departamento de Cundinamarca, en la sede de la Empresa de Servicios Públicos de Chía "EMSERCHÍA E.S.P., ubicada en la calle 11 No. 17 - 00.

SUPERVISIÓN

La supervisión del contrato será realizada por el PROFESIONAL UNIVERSITARIO SISTEMAS DE INFORMACIÓN ADSCRITO A LA OFICINA ASESORA DE PLANEACIÓN o quien haga sus veces.

DESCRIPCIÓN TÉCNICA DEL OBJETO A CONTRATAR Y OBLIGACIONES ESPECIALES DEL CONTRATISTA

OBLIGACIONES ESPECIFICAS

ITEM	CANTIDAD	DESCRIPCION

1	100	**Suscripción al servicio de protección al correo, por un (1) añoHarmony Advanced Email,** Advanced Anti-Phishing, including URL inspection and file sandboxing andsanitization (CDR), for incoming and internal Office 365 and Google Suite emails for 1 year&. Anti-Phishing for incoming and internal emails&. Complete known malware and zero-day malware prevention (Sandboxing)&. Attachment sanitization (CDR; Threat Extraction)&. Malicious URL protection (URL Protection)&. URL Click-Time Protection (URL Re-writing)&. Account takeover prevention (Anomalies)&. Unauthorized applications detection (Shadow IT)Incluye soporte directo con fabricante, en horario de atención: 5x9, de Lunes a Viernes, no incluye festivos
2	1	Servicio de configuración El alcance del servicio comprende:• Análisis inicial de la infraestructura y recolección de información• Activación de la consola de administración en la nube• Integración con el dominio de correo existente.• Creación de políticas, hasta 10 reglas de seguridad, aplicadas a grupos de usuarios o al dominio completo• Configuración de templates para la generación de hasta 3 reportes personalizados• Configuración de cuentas de gestión adicionales • Integración con el dominio de correo existente.• Puesta en marcha de la solución.• Transferencia de conocimientos de 4 horas
3	1	Servicio de soporte local, basado en Banco de hasta 10 horas El alcance del servicio comprende:• Horario de atención: 5x8 de Lunes a Viernes, no incluye festivos• Atención remota• Atención de casos relacionados con fallas (soporte correctivo)• Atención de casos no relacionados con fallas, como nuevas configuraciones, cambios, transferencias de conocimientos, etc.• El conteo de las horas se realizará en unidades, no fracciones. Vigencia: un año

OBLIGACIONES GENERALES:

1. Cumplir con las instrucciones impartidas por el funcionario encargado del control y vigilancia del contrato y las demás que sean inherentes al objeto de la presente contratación.
2. El contratista deberá presentar los comprobantes de pago de las obligaciones parafiscales, de conformidad con el Artículo 9 de la Ley 828 de 2003, y el Artículo 23 de la Ley 1150 de 2007.
3. Defender en todas sus actuaciones los intereses de la Empresa De Servicios Públicos de Chía EMSERCHIA E.S.P. con lealtad y buena fe en todas las etapas contractuales.
4. Adelantar los trámites y cumplir los requisitos para la ejecución del contrato dentro de los plazos establecidos.
5. Informar oportunamente de cualquier petición, amenaza de quien actuando por fuera de la ley pretenda obligarlo a hacer u omitir algún acto u ocultar hechos que afecten los intereses de la Empresa de Servicios Públicos de Chía "EMSERCHÍA E.S.P.", del Municipio de Chía o de alguna sus dependencias.
6. Cumplir con los plazos establecidos en este contrato y en particular con las demás inherentes.
7. Realizar apoyo a todas las actividades y acciones que adelante EMSERCHÍA E.S.P.
8. Cumplir con las instrucciones impartidas por el Supervisor del contrato designado por la Empresa.
9. Todas las demás inherentes o necesarias para la correcta ejecución del objeto contractual.

CERTIFICACIÓN QUE NO EXISTE CONTRATO CELEBRADO EN LA ACTUALIDAD CON EL MISMO OBJETO Y OBLIGACIONES
Que en la actualidad, EMSERCHÍA E.S.P. NO cuenta con una herramienta para evitar ataques a las aplicaciones SaaS para bloquear a los ciberdelincuentes a los diferentes ataques como Malware , Phishing, robo de credenciales y fuga de datos a través de nuestro correo corporativo, por lo tanto se requiere de la contratación del bien y/o servicio según el objeto a contratar y la descripción técnica y obligaciones especiales del contratista.
MODALIDAD DE SELECCIÓN
CONTRATACIÓN DIRECTA ☒
FUNDAMENTOS JURÍDICOS DE LA MODALIDAD DE SELECCIÓN
La contratación se regirá por lo dispuesto en la Ley 142 de 1994, Ley 689 de 2001, Acuerdo de Junta Directiva No. 005 de 2022, por el cual se aprueba el manual de procedimientos para la contratación en la Empresa de Servicios Públicos de Chía EMSERCHÍA E.S.P, Resolución 551 de 2022 por medio de la cual se adopta el manual de procedimientos para la contratación en la Empresa de Servicios Públicos de Chía EMSERCHÍA E.S.P, y la Ley 80 de 1993, en lo referente a los principios de la contratación y el Código de Comercio. En el Acuerdo de Junta Directiva No. 005 de 2022, por el cual se aprueba el manual de procedimientos para la contratación en la Empresa de Servicios Públicos de Chía EMSERCHÍA E.S.P, y la Resolución 551 de 2022 por medio de la cual se adopta el manual de procedimientos para la contratación en la Empresa de Servicios Públicos de Chía EMSERCHÍA E.S.P, sección II, capítulo I del título II, se establecen los procedimientos que habrá de utilizarse para escoger al contratista. Teniendo en cuenta el objeto SUSCRIPCION A LA HERRAMIENTA HARMONY EMAIL CON EL FIN DE PROTEGER LOS CORREOS ELECTRONICOS CONTRA PHISHING Y MALWARE PARA LA EMPRESA DE SERVICIOS PUBLICOS DE CHIA EMSERCHIA E.S.P cuyo presupuesto oficial de la contratación asciende a la suma de Diecisiete millones cuatroscientos sesenta mil pesos MCTE ($ 17.460.000), el procedimiento de selección que ha de surtirse es CONTRATACIÓN DIRECTA, con observancia de los principios de la contratación establecidos en el numeral 3, Capítulo I del Título I del Acuerdo de Junta Directiva 005 de 2022 por el cual se aprueba el manual de procedimientos para la contratación en la Empresa de Servicios Públicos de Chía EMSERCHÍA E.S.P y Resolución 551 de 2022 por medio de la cual se adopta el manual de procedimientos para la contratación en la Empresa de Servicios Públicos de Chía EMSERCHÍA E.S.P y criterios de eficacia y eficiencia.

ANÁLISIS ECONÓMICO - MÉTODO UTILIZADO				
PRECIOS DEL MERCADO ☐	PRECIOS REGULADOS ☐	PRECIOS Y DATOS HISTORICOS ☐	FUENTES DE INFORMACIÓN OFICIALES O GUBERNAMENTALES ☐	OTROS ☒
DESARROLLO Y EXPLICACIÓN	Para efectos de determinar el valor del contrato, se consideran los precios del mercado, calidad de los productos y servicio analizando las condiciones de 3 cotizaciones solicitadas para la prestación del servicio, y se escoge la de menor valor.			

ANÁLISIS DE LOS RIESGOS PREVISIBLES DEL FUTURO CONTRATO.

Se deberá analizar cuál de los siguientes riesgos impacta en el objeto de la contratación:

TIPIFICACIÓN		ESTIMACIÓN	IMPACTO	ASIGNACIÓN
TIPO DE RIESGO	DESCRIPCIÓN DEL RIESGO			
ECONÓMICOS	Fluctuación de los precios de los insumos	Poco Probable	BAJO	CONTRATISTA
	Desabastecimiento y especulación de precios	Poco Probable	BAJO	CONTRATISTA
	Alteraciones por el comportamiento de la moneda	Poco Probable	BAJO	CONTRATISTA
SOCIALES O POLÍTICOS	Cambios de las políticas gubernamentales que sean probables y previsibles que tengan impacto en la ejecución del contrato	Poco Probable	BAJO	CONTRATISTA
	Paros, huelgas, actos terroristas que incidan en la ejecución del contrato	Poco Probable	BAJO	CONTRATISTA - CONTRATISTA
OPERACIONALES	Posibilidad de que el monto de la inversión no sea el previsto para cumplir el objeto del contrato.	Poco Probable	BAJO	EMPRESA
	Extensión del plazo, cuando los contratos se realizan en tiempos distintos a los inicialmente programados por circunstancias no imputables a las partes.	Poco Probable	BAJO	CONTRATISTA-EMPRESA
	Posibilidad de no obtención del objeto del contrato como consecuencia de la existencia de inadecuados procesos, procedimientos, parámetros, sistemas de información y tecnológicos, equipos humanos o técnicos sin que los mismos sean imputables a las partes.	Poco Probable	BAJO	CONTRATISTA
FINANCIEROS	Dificultad de conseguir los recursos financieros, ya sea en el sector financiero o el mercado de capitales, para lograr el objetivo del contrato.	Poco Probable	BAJO	CONTRATISTA
	Variaciones o fluctuaciones en tasas de interés o condiciones del mercado que afecten los flujos futuros del contratista.	Poco Probable	BAJO	CONTRATISTA

REGULATORIOS	Son los posibles cambios regulatorios o reglamentarios que siendo previsibles, afecten el equilibrio contractual.	Poco Probable	BAJO	EMPRESA
DE LA NATURALEZA	Eventos causados por la naturaleza sin la intervención o voluntad del hombre, que aunque pueden ser previsibles por su frecuencia o diagnóstico están fuera del control de las partes.	Poco Probable	BAJO	CONTRATISTA
AMBIENTALES	Se refiere a las obligaciones que emanan de las licencias ambientales, de los planes de manejo ambiental, de las condiciones ambientales o ecológicas exigidas y de la evolución de las tasas retributivas y de uso del agua. Como en el caso que durante la ejecución del contrato se configuren pasivos ambientales causados por mala gestión de la licencia ambiental y/o el plan de manejo ambiental o el costo de las obligaciones ambientales resulte superior al estimado no siendo imputables a las partes.	Poco Probable	BAJO	CONTRATISTA
TECNOLÓGICOS	Eventuales fallos en las telecomunicaciones, suspensión de servicios públicos, advenimiento de nuevos desarrollos tecnológicos o estándares que deben ser tenidos en cuenta para la ejecución del contrato así como la obsolescencia tecnológica.	Poco Probable	BAJO	CONTRATISTA

GARANTÍAS CONTRACTUALES

GARANTÍA ÚNICA DE CUMPLIMIENTO

Para garantizar el cumplimiento general de las obligaciones derivadas del contrato, los oferentes deben comprometerse a constituir garantía dentro de los cinco (5) días hábiles siguientes a la firma del contrato y a favor de EMSERCHÍA E.S.P., mediante la cual se ampare:

APLICA		RIESGO ASEGURADO	MONTO ASEGURADO	VIGENCIA	BENEFICIARIOS
SI	NO				
	X	Anticipo del 30% al 50%	100% del valor del anticipo	Por un término igual al contrato y 4 meses más	Entidad Contratante
X		Cumplimiento de las Obligaciones del Contrato	20% del valor del contrato	Por un término igual al contrato y 6 meses más	Entidad Contratante
	X	Calidad de bienes o servicios	20% al 30% del valor del contrato	Por un término igual al contrato y 1 año más	Entidad Contratante
	X	Salarios y Prestaciones Sociales	20% del valor del contrato	Por un término igual al contrato y 3 años más	Contratante y trabajadores del contratista
	X	Responsabilidad Civil Extracontractual	20% al 30% del valor del contrato	Por un término igual al contrato.	Contratante y Eventuales víctimas
	X	Estabilidad de Obra	10% al 30% del valor del contrato	Por un término igual al contrato y 5 años más	Entidad Contratante
	X	Calidad de los Materiales de la Obra Pública	20% del valor del contrato	Por un término igual al contrato y 1 año más	Entidad Contratante

El término de la Garantía Única correrá a partir de la fecha de vigencia del amparo y estará sujeta a la aprobación de EMSERCHÍA E.S.P. y no expirará por falta de pago de la prima o revocatoria unilateral.

Si la compañía de seguros establece en las pólizas algún porcentaje como deducible y lo hace efectivo en caso de siniestro, el mismo será asumido por el CONTRATISTA. En caso de póliza de seguro, esta debe adjuntarse acompañada de las condiciones generales.

La empresa podrá ordenar al proponente ampliación del valor asegurado cuando luego de las correcciones aritméticas resulte un valor superior al inicialmente propuesto. Igualmente podrá solicitar la ampliación de la vigencia cuando las necesidades de la empresa exijan la ampliación del plazo para adjudicar.

Si el proponente es una persona jurídica, la póliza o garantía deberá constituirse con el nombre o razón social que figura en el Certificado de Existencia y Representación Legal expedido por la Cámara de Comercio respectiva, y no sólo con su sigla, a no ser que en el referido documento se exprese que la sociedad podrá denominarse de esa manera. Cuando la propuesta se presente en Consorcio o Unión Temporal, la póliza deberá constituirse a nombre de todos sus integrantes, y no a nombre de los representantes legales.

La póliza deberá presentarse debidamente firmada por el tomador y con el recibo de caja o certificación de pago de la misma.

FIRMA:
ELABORADO POR: HUMBERTO BARAJAS LOPEZ
CARGO: P.U. Sistemas De información
Revisión: Lizeth Alexandra Rodríguez Rozo – Jefe Oficina Asesora De Planeación