empocaldas	F-GC-01 Versión: 10 Enero 2019	Empresa de Obras Sanitarias de Caldas EMPOCALDAS S.A. E.S.P. ESTUDIO DE NECESIDAD DE CONTRATACIÓN

Fecha del estudio lunes, 28 de enero de 2019

Objeto de la contratación FORTALECIMIENTO DEL SISTEMA DE PROTECCION CONTRA ATAQUES INFORMATICOS A LA EMPRESA

VERIFICACIONES PREVIAS

Requerimiento previo No aplica

DESCRIPCIÓN DE LA NECESIDAD Y OPORTUNIDAD

Necesidad

La empresa EMPOCALDAS S.A. E.S.P necesita implementar sistemas de seguridad avanzados para accesos de alto rendimiento, de alta seguridad, alta disponibilidad para ayudar a garantizar la continuidad del negocio, un sistema que pueda ser capaz de verificar tanto interna como externamente la red, analizando cada capa de la misma, no sólo a nivel de puertos de servicios, blindando los segmentos definidos por el equipo IT, obteniendo seguridad inteligente, debe hacer revisión de los ataques y comportamientos no habituales dentro de cada red que se proteja, adicionalmente debe mostrar en el tiempo los comportamientos de los ataques granular mente y emitir alertas para tomar medidas, esto genera continuidad en la empresa, no solo revisar dispositivos de red comunes como equipos pc, permite detectar amanazas avanzadas de Malware, control de aplicaciones e inspección IPS.
Debe ser capaz de analizar máquinas virtuales, dispositivos móviles, diferentes sistemas operativos, impresoras, routers y switch, sistemas de telefonía, sistemas de servidores, protocolos de aplicaciones http, ssh, smtp, en aplicaciones web. Debe permitir generar alertas y recibir alertas a nivel de bases de datos, debe ser capaz de analizar un comportamiento sencillo como malware, antispam detrás de los archivos temporales, debe garantizar la protecciòn tecnològica de todo el Dominio de la red Empocaldas, tambièn debe tener las condiciones tècnicas de protecciòn y seguridad en hardware, software y licencias que le garanticen a la empresa Empocaldas el normal funcionamiento en sus sistemas de informaciòn y procesos Tecnològicos, como tambièn el ofrecer la protecciòn en el crecimiento tecnològico que se està teniendo actualmente en la nube de internet, donde se deben realizar configuraciones adicionales con las plataformas de los terceros donde Empocaldas S.A. E.S.P. tiene y està iniciando nuevos servicios; la seguridad tecnològica es uno de los pilares fundamentales y el proponente del objeto de este estudio de necesidad de contratación, es la actualizaciòn de la plataforma de seguridad con todas las configuraciones tecnològicas que se necesitan actualmente para garantizar el normal funcionamiento de los sistemas que se prestan dentro del Dominio de Empocaldas, seccionales, plantas de tratamiento, como tambièn los servicios que se tienen en Outsourcing, pero se debe garantizar la seguridad tecnològica porque la informaciòn es un activo vital para las empresas y deben definirse las estrategias de seguridad para garantizar los procesos.
La solución debe incluir la nueva generación IPS (NGIPS) que ofrece prevención muy eficaz contra amenazas y la conciencia contextual completa de los usuarios, la infraestructura, las aplicaciones y el contenido para detectar amenazas multivectoriales y automatizar la respuesta de defensa. El sistema debe incluir un sistema para el Filtrado de URL basado en reputación, y basado en categorías de alertas y debe ofrecer un amplio control sobre el tráfico web sospechoso y hacer cumplir las políticas en cientos de millones de URLs en más de 80 categorías. El sistema debe ofrecer una avanzada protección contra malware y antispam con comprobada eficacia, debe ser líder en la industria de detección de incumplimiento, con un TCO bajo, y el valor de protección superior que le ayuda a descubrir, entender y detener el malware, antispam y las amenazas emergentes perdidas por otras capas de seguridad.
La solución tiene que proporcionar a los equipos de seguridad una visibilidad completa y control sobre la actividad dentro de la red. Dicha visibilidad incluye usuarios, dispositivos de comunicación entre máquinas virtuales, las vulnerabilidades, las amenazas, las aplicaciones del lado del cliente, archivos y sitios web. El sistema de Centro de Gestión debe proporcionar un conocimiento de contenido con trayectoria de archivos de malware y antispam que ayude a detener la infección y a

detectar la causa raíz para acelerar el tiempo de solución. El sistema debe estar especialmente diseñado para ser altamente escalable, alcanzar velocidades de hasta multigigabit, y proporciona seguridad coherente y sólida en toda la rama, con el borde de Internet y centros de datos en entornos físicos y virtuales.

El sistema de gestión debe analizar líneas corrientes para correlacionar las amenazas, evaluar su impacto, de forma automática la política de seguridad se debe ajustar y detectar las identidades de los usuarios que ocasionan los eventos de seguridad. El sistema debe continuamente monitorear la red y como cambia con el tiempo. Las nuevas amenazas deben ser evaluadas automáticamente para determinar lo que puede afectar el negocio. El proveedor de la solución debe tener relacionamiento directo con el fabricante, donde debe definirse mínimo como canal Cisco Select, y debe tener soporte en sitio, suministrando apoyo de ingeniería con personal certificado CCNA1, IT, cableado estructurado en varios fabricantes. Tambièn deberà certificar experiencia en el montaje de equipos de seguridad Cisco. Para la actualizaciòn de la plataforma de seguridad, el proponente deberà cumplir con un equipo de trabajo especializado y certificado

Conveniencia

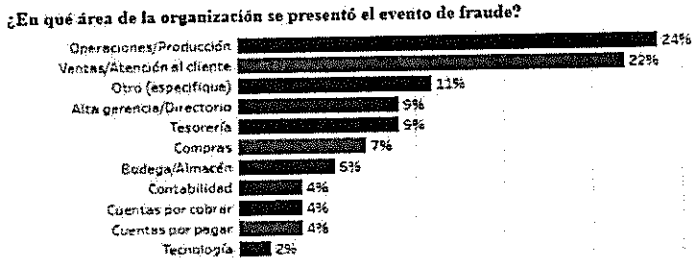
Realizar la actualizaciòn de la plataforma de Seguridad en los siguientes vectores: correo electrónico office 365, sistema de protecciòn DNS, protecciòn avanzada contra Malware y refuerzo en política se seguridad en las seccionales; es conveniente para la organización, porque le ayuda a la empresa a ser más eficaz en sus actividades, lograr mejores índices de desempeño cada día; tambièn las plataformas tecnológicas son herramientas que ayudan en la administraciòn de procesos, el logro de objetivos estrategicos; tambièn son fundamentales para apoyar a las empresas en el crecimiento tecnològico el cual es un reto de todos los administradores de tecnologìa.

Oportunidad

Es oportuno garantizar el normal funcionamiento de todos los sistemas y plataformas de TI de la empresa, realizando un fortalecimiento en la protecciòn contra ataques informáticos durante la presente vigenica, toda vez que se encuentran documentados en la prensa nacional, ataques a Empresas y entidades oficiales en sus procesos informáticos y de Tesorería así:

- Desarticulan organización que se apropió de 800 millones del Fondo de Vigilancia de Bogotá Sustrajeron, mediante dos transacciones, la suma de $ 808.642.000, direccionados a 38 personas. Realizada la investigación, se encontró que del computador de tesorería –único habilitado para hacer transacciones– se sustrajo información que permitió el fraude. La fuente de la noticia es la siguiente: http://www.wradio.com.co/noticias/judicial/desarticulan-organizacion-que-se-apropio-de-800-millones-del-fondo-de-vigilancia-de-bogota/20181116/nota/3825247.aspx
- Planeaban robar $1.040 millones a la Universidad de Caldas, Martes, Diciembre 11, 2018, Gracias al llamado de la entidad financiera se logró desautorizar el movimiento financiero. En un comunicado, la institución educativa manifestó que denunció ante las autoridades el intento de robo a través de un ataque informático por $1.040 millones. Los hechos ocurrieron ayer. Según el texto, cibercriminales trataron de realizar una transacción desde una cuenta bancaria de la Universidad a una particular. http://www.lapatria.com/sucesos/planeaban-robar-1040-millones-la-universidad-de-caldas-428403

De acuerdo con la firma KPGM en su Encuesta de Fraude en Colombia 2017, https://public.tableau.com/profile/kpmgco#!/vizhome/EncuestadeFraudeenColombia2017/Historia1, el siguiente es el pefil de raude en Colombia, donde los fraudes electrónico aparece como una d elas principales causas.



REQUISITOS TÉCNICOS Y LEGALES DEL BIEN O SERVICIO

Aspectos Técnicos del Bien y/o Servicio

El proponente deberà cumplir con la siguientes licencias en la actualizaciòn para el sistema de protecciòn contra ataques informacticos a la empresa EMPOCALDAS S.A. E.S.P.

QTY	DETALLE
	LICENCIAS DE ANYCONNECT

1	Cisco AnyConnect Plus Term License - 36 Meses Paquete de 250 licencias
	PROTECCION DE DNS Y AMP
1	UMBRELLA -INSIGHTS 36 MESES SERVICIO DE SEGURIDADAD CLOUD CISCO - 250 Licencias
1	AMP FOR END POINT - PROTECCION HASTA 65 ESTACIONES CRITICAS Cisco CES Advanced Malware Protection 3YR
	PROTECCION DE EMAIL 0365
1	Protección de seguridad para el trafico de Email para correo entrante + AMP, con cubrimiento para 323 cuentas SERICIOI DE PROTECCION CLOUD CISCO PARA CORREO 365 DURANTE 36 MESES AntiSpam (IPAS), Anti-Virus (Sophos), Outbreak Filters, Central Mgmt & Reporting Cloud Email Security AMP Add-on SVP Cloud Email Security Inbound Essentials License SVP Cloud Email Security Inbound Essentials License Cisco CES Inbound Essentials Bundle 3YR, 200-499 Users

Ítem	Código Inventario	Cód Nac. Unidas	Descripción del Bien o servicio	Unidad	Cantidad
		81111801	Seguridad de los computadores, redes o internet		

EXPERIENCIA REQUERIDA

Condiciones de idoneidad y experiencia que llevan a contratar a la persona natural o jurídica	El oferente deberá contar con certificación del fabricante Cisco en la cual se especifique partner de Cisco mínimo Select, autorizado para adquirir, distribuir e implementar productos y servicios en el territorio colombiano.

SOPORTE DE PRECIOS DEL MERCADO

Persona Natural y jurídica	Contacto	Email	Teléfono	Valor cotización
Data y Service	Jonathan Rodríguez Paipa	contactenos1@datayservice.com	316-7421195	127.115.071
		Total precio de mercado		127.115.071

Adjuntar soportes de precio de mercado.
Todos los precios deben incluir IVA
En caso de no adjuntar los soportes de precio de mercado, deberá adjuntar constancia de las condiciones de calidad o idoneidad del oferente, con su respectiva cotización.

PRESUPUESTO

Vigencia actual	Vigencia futura	Total
2019	2020	Total vigencias
127.115.071	-	127.115.071

Cod. Rubro	Nombre Rubro de apropiación	Valor de la apropiación
21020225	Sistematizaciòn	127.115.071
	Total CDP	127.115.071

Centro de costos
11205 - MANIZALES SISTEMAS

OBLIGACIONES GENERALES DEL CONTRATISTA

Obligación	Aplica
Cumplir con todas las especificaciones y requerimientos del Estudio de Necesidad de la contratación y aspectos contemplados en la solicitud de oferta.	Sí aplica
El contratista deberá concertar con el supervisor un cronograma de actividades o plan de entregas de acuerdo al objeto del contrato y las necesidades de la Empocaldas S.A. E.S.P..	Sí aplica
Asumir por su cuenta y riesgo todos los gastos en el desarrollo del contrato.	Sí aplica
Presentar el pago de aportes a la seguridad social cada mes al supervisor del contrato con el fin de autorizar el pago correspondiente.	Sí aplica
En caso de tener trabajadores a cargo deberá suministrar los elementos de protección requeridos para el desarrollo de su función y asegurarse de que los usen.	Sí aplica
Cumplir con el protocolo de seguridad que se establezca para el ingreso a Empocaldas S.A. E.S.P. y los frentes de trabajo de la misma, y la seguridad de los datos que se procesen, verificando que no existan fugas ni indebido uso de la información.	Sí aplica
Sin perjuicio de la autonomía técnica y administrativa, atender instrucciones y lineamientos que durante el desarrollo del contrato se le impartan por parte de la Empocaldas S.A. E.S.P. (Supervisor). Como presentar los informes que se exija.	Sí aplica
Contar con un formato de pedido sistematizado por área que permita atender solicitudes valoradas para cada uno de los centros de costo. (Centro de costos en unidades y en pesos, consumo en unidades y valor, facturación total y detallada por cada centro de costos, trazabilidad de tubería, por medio físico y magnético)	Sí aplica
El proveedor debe estar dispuesto a atender los requerimientos de los centros de costos en fechas previamente establecidas con el supervisor.	Sí aplica
En el evento que algún o algunos de los elementos sea rechazado por el supervisor del contrato, dichos productos deberán ser retirados por cuenta y riesgos del contratista a la mayor brevedad posible. (o en el tiempo indicado en la invitación) El contratista deberá corregir cualquier problema que se presente, respondiendo por partes dañadas, por su cuenta y riesgo durante la garantía.	No aplica
Responder por los daños que ocasione en desarrollo del contrato a Empocaldas S.A. E.S.P. y a terceros afectados.	Sí aplica
Presentar al supervisor del contrato de Empocaldas S.A. E.S.P., un plan de manejo ambiental, en caso de generarse algún residuo sólido, líquido o gaseoso con ocasión de la ejecución del contrato, donde describa los residuos que generará y el aprovechamiento o la disposición final de los mismos.	No aplica
Garantizar el cumplimiento de los requisitos de calidad de la norma ISO 9001 determinados por el Empocaldas S.A. E.S.P.. (Para los eventos de ejecutar trabajos en las plantas que pueda afectar la calidad del agua o del proceso de tratamiento, deberá contar con autorización por parte del Administrador de la seccional).	No aplica
Informar oportunamente al supervisor del contrato, los inconvenientes en la entrega de los bienes objeto de suministro y proponer soluciones para garantizar la prestación del servicio.	Sí aplica
Las demás obligaciones a su cargo que se deriven de la naturaleza del contrato y de las exigencias legales.	Sí aplica

OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

Las obligaciones específicas a cargo del contratista serán las siguientes:	Aplica
El oferente deberá contar con certificación del fabricante Cisco en la cual se especifique partner de Cisco mínimo Select, autorizado para adquirir, distribuir e implementar productos y servicios en el territorio colombiano	Sí aplica

<table>
<tr><td colspan="2">El oferente deberá certificar experiencia en el montaje de equipos de seguridad de Cisco (anexar al menos 1 certificado de experiencia): •ASA Cisco, •FirePower Services, •Any connect</td><td>Sí aplica</td></tr>
<tr><td colspan="2">Equipo de Trabajo: El oferente deberá contar con un equipo conformado de la siguiente forma</td><td>Sí aplica</td></tr>
<tr><td>Responsable de la Capa de Networking</td><td>Persona con una experiencia mínima de dos (2) años, profesional en ingeniería electrónica o afines</td><td rowspan="3">Sí aplica</td></tr>
<tr><td>Certificaciones</td><td>Cisco Certified Network Associate (CCNA)
ITIL Foundations</td></tr>
<tr><td>Objetivo</td><td>Planear la integración e implementación de la solución ofertada a nivel de Networking y centro de datos.</td></tr>
<tr><td>Responsable de la Seguridad</td><td>El personal encargado de la plataforma de seguridad en la nube.</td><td rowspan="2">Sí aplica</td></tr>
<tr><td>Certificaciones</td><td>Security – System Engineers – Essentials
Security – System Engineers – Network Security
Security – System Engineers – Advanced Threat
Security – System Engineers – Visibility
Security – System Engineers – Cloud, Web</td></tr>
<tr><td>Equipo de Ingeniería</td><td>El equipo de ingeniería debe contar mínimo con los siguientes requisitos:</td><td rowspan="8">Sí aplica</td></tr>
<tr><td>Cisco</td><td>Mínimo un ingeniero con dos (2) años de experiencia, profesional en ingeniería electrónica o afines.</td></tr>
<tr><td>certificaciones y/o especializaciones en cisco:</td><td>Security – System Engineers – Essentials
Security – System Engineers – Network Security
Security – System Engineers – Advanced Threat
Security – System Engineers – Visibility
Security – System Engineers – Cloud, Web</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Profesional en Ingenieria</td><td>Persona con una experiencia mínima de dos (2) años, profesional en ingeniería de sistemas y telecomunicaciones, que tenga las siguientes certificaciones:</td></tr>
<tr><td>Certificaciones</td><td>ISACA. Certified Information Security Manager – CISM,
Fortinet NSE 4 Security Profesional.</td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="3">Responsable del Plan de Adopción de la Infraestructura</td><td>Se requiere una persona encargada para desplegar el proceso de adopción de la infraestructura a implementar, la cual deberá estar localizada en Manizales, con las siguientes funciones:</td></tr>
<tr><td>1.Identificar los usuarios impactados con la renovación tecnológica que se encuentran dentro de la compañía</td></tr>
<tr><td>2.Construir campañas de capacitación
Identificar las necesidades de capacitación de acuerdo con los cambios realizados dentro la infraestructura de la compañía.
Realizar cronograma de actividades para capacitación
Ejecutar el plan de capacitaciones</td></tr>
<tr><td colspan="2">El oferente se hará responsable de los salarios, prestaciones sociales, seguridad social del personal que elabore el mantenimiento preventivo o correctivo de los equipos instalados en la empresa, IVA, Retención en la fuente y demás costos que implique la ejecución del contrato.</td><td>Sí aplica</td></tr>
<tr><td colspan="2">El oferente deberá constituir las pólizas que son exigidas en el Contrato.</td><td>Sí aplica</td></tr>
<tr><td colspan="2">El oferente debe adjuntar fichas técnicas de todos los elementos de hardware ofrecidos, los cuales deben ser iguales en marcas, líneas y características técnicas a los ofrecidos en la propuesta aportada por el oferente.</td><td>Sí aplica</td></tr>
<tr><td colspan="2">El oferente entregará un Plan de trabajo y la metodología de implementación de la solución adquirida.</td><td>Sí aplica</td></tr>
<tr><td colspan="2">El oferente diseñará el Plan de contingencia y rollback para garantizar el normal funcionamiento de la plataforma de seguridad perimetral</td><td>Sí aplica</td></tr>
<tr><td colspan="2">El oferente entregará los Diagramas de la plataforma, integración con terceros de la seguridad perimetral de ser necesario para garantizar el normal funcionamiento y operación de todos los servicios</td><td>Sí aplica</td></tr>
</table>

Entrega de todos los componentes de hardware y software funcionando de acuerdo con lo solicitado por Empocaldas.	Sí aplica
El oferente entregará documentación del hardware y software, tales como manuales de administración, configuración y parametrización y demás elementos necesarios para su completa operación	Sí aplica
El oferente entregará licenciamiento de todos los productos de la plataforma de seguridad perimetral con las garantías	Sí aplica
El oferente identificará los diferentes grupos de usuario dentro de la organización los cuales consumirán el recurso tecnológico, también diseñarán el plan de adopción para los diferentes grupos de usuarios identificados dentro de la compañía y realizarán las campañas de sensibilización y reinducción.	Sí aplica
Se debe realizar el bloqueo de malware, botnets y pishing sobre cualquier puerto, protocolo o aplicación. Permitir detener oportunamente el phishing y las infecciones de malware, identificar dispositivos que ya han sido infectados ayudando a prevenir la sustracción de datos.	Sí aplica
Obtener visibilidad a nivel de solicitudes de tipo DNS de toda la actividad que se registra en internet en diferentes ubicaciones, dispositivos y usuarios.	Sí aplica
El servicio de protección de DNS se debe proveer y administrar desde la nube.	Sí aplica
Permitir bloquear proactivamente solicitudes a destinos que sean considerados maliciosos antes de establecer una conexión.	Sí aplica
La protección DNS no debe añadir latencia adicional al usuario final.	Sí aplica
Obtener una primera línea de defensa contra las amenazas en internet, sin importar la ubicación de los usuarios.	Sí aplica
Analizar las solicitudes DNS y determinar si son seguras, maliciosas o peligrosas, tomando acciones determinadas para cada caso (bloquear, permitir, analizar)	Sí aplica
Detectar y supervisar el malware de manera inmediata y de manera retrospectiva.	Sí aplica
Proteger diferentes dispositivos con la solución de antimalware (PC, Mac, Dispositivos móviles y entornos virtuales)	Sí aplica
Permitir registrar actividad de los archivos a lo largo del tiempo para poder rastrear la difusión del malware.	Sí aplica
Permitir detectar, contener y remediar las amenazas que consigan eludir la primera línea de defensa.	Sí aplica
Permitir identificar software vulnerable que puede ser blanco de ataques de cada uno de los hosts, como también potenciales vulnerabilidades de seguridad.	Sí aplica
Indicar cuales son los Hosts que requieren que se apliquen parches.	Sí aplica
Permitir llevar a cabo un seguimiento continuo de las actividades que se encuentran en ejecución y las comunicaciones de un determinado host para entender las principales causas que llevan a tener un riesgo de seguridad	Sí aplica
La herramienta de Antimalware debe tener visibilidad de los archivos que se están ejecutando a nivel generar en la organización por orden de prevalencia, lo que permite detectar amenazas.	Sí aplica
Se debe poder realizar análisis de malware dinámico, ejecutando malware en un entorno controlado y comparando su comportamiento con un conjunto de indicadores. Esto podrá permitir detectar amenazas de día cero.	Sí aplica
Detener comunicaciones de "callback" en el punto de origen (incluyendo dispositivos finales que se encuentren fuera de la organización.	Sí aplica
La solución de antimalware debe estar basada en la nube.	Sí aplica
Obtener una protección a nivel del correo electrónico de la compañía que se encuentra actualmente operativo en la nube (Exchange O365).	Sí aplica
La herramienta de protección de correo debe tener las siguientes características: •Filtros anti-Spam •Protección con Antivirus •Aplicación de políticas por filtrado de contenido •Protección Malware avanzado •Seguimiento de correos •Encripción de correo •Reporte detallado •Detección de correo gris (correos no deseados de marketing, social media, mensajes masivos). Bloqueo de remitentes fraudulentos	Sí aplica
La herramienta de protección de correo debe estar basado en la nube y debe integrarse con O365.	Sí aplica
Obtener protección contra ramsomware, compromisos de seguridad del correo electrónico, suplantación de identidad.	Sí aplica

Permitir detener amenazas basadas en URL antes de que se reciban en la bandeja de entrada de los usuarios finales.	Sí aplica
Integrar la solución con la nube de Talos, lo que permite tener una actualización constante de todos los eventos de seguridad que suceden a nivel mundial.	Sí aplica
Permitir realizar conexión de VPN de un número determinado de usuarios finales.	Sí aplica
Mantener usuarios móviles con detección de red segura, lo que permite reconocer cuando se debe activar AnyConnect.	Sí aplica
Simplificar la autenticación de usuarios y dispositivos.	Sí aplica
Reducir las desconexiones de las aplicaciones para los usuarios con la funcionalidad de reconexión automática en caso de que la conexión de red se pierda.	Sí aplica
Debe permitir soporte para diferentes dispositivos y plataformas. (Mac, Windows, dispositivos móviles)	Sí aplica
Permitir integración con las diferentes herramientas de seguridad de Cisco (AMP, herramienta de protección de DNS)	Sí aplica

OBLIGACIONES ESPECIFICAS DE EMPOCALDAS

Las obligaciones específicas a cargo de Empocaldas S.A. E.S.P. serán las siguientes:	Aplica
Pago oportuno de las obligaciones contraídas con el contratista, después del visto bueno del supervisor del contrato 30 días después.	Sí aplica
Entrega de certificaciones y demás documentos solicitados por el contratista para el óptimo desarrollo del Contrato.	Sí aplica

LUGAR Y PLAZO DE EJECUCIÓN

Lugar de ejecución	Seccional principal Ciudad de Manizales, Departamento de Caldas, Colombia, donde Empocaldas S.A. E.S.P. tiene instalada la plataforma tecnològica; pero el cubrimiento es para toda la infraestructura tecnològica de la empresa.
Plazo de ejecución	30 dias calendario contados desde la suscripción de acta de inicio.

FORMA DE PAGO

Forma de Pago	En forma parcial conforme a las actas presentadas y aprobadas por el supervisor.
Condiciones para Pago	El contratista entiende que en virtud de la ordenanza 816 del 22 de Diciembre de 2017 de la Asamblea Departamental de Caldas, el recaudo sobre las estampillas se efectuará mediante retención sobre los anticipos, pagos parciales, pagos o abonos en cuenta; por lo tanto el contratista autoriza con la firma del presente contrato y/o carta de presentación de la oferta para que la Empocaldas S.A. E.S.P. efectué los descuentos correspondientes por el monto equivalente al valor de las estampillas 1. Presentación de la factura 2. Certificación del almacén de la entrada del insumo y visto bueno del supervisor. 3. Certificado de cumplimiento expedido por el supervisor. 4. Certificado o planilla del pago de aportes de seguridad social y/o aportes parafiscales según corresponda. 5. Las demás que requiera el supervisor del contrato y la lista de chequeo de Empocaldas S.A. E.S.P.

Estampilla a descontar	Aplica
Estampilla Pro Universidad (1%)	Sí aplica
Estampilla Pro Desarrrollo (2%)	Sí aplica
Estampilla Pro Hospital (1%)	Sí aplica
Estampilla Pro Adulto mayor (3%)	Sí aplica
Contribución Especial (5%)	No aplica

ASIGNACION Y DISTRIBUCIÓN DEL RIESGO

Riesgo
Está a cargo de contratista, el incremento de precios de los elementos relativos a la materia prima para producir el bien a adquirir a nivel nacional e internacional.
Está a cargo del contratista el riesgo comercial, entendido como los eventos desfavorables relacionados con el valor y pago del contrato, causados por variaciones en las condiciones del mercado, aumento en los factores de producción, en el valor de los insumos o de los fletes
Está a cargo del contratista el riesgo país, entendido como el cambio de las políticas en el país de origen.
Está a cargo del contratista el riesgo operativo, entendido como los eventos relacionados con los procesos de producción, transporte y entrega del producto, tales como: Falta de disponibilidad de Materia Prima, insuficiente capacidad de producción, retrasos en el tiempo de entrega, incumplimiento en los protocolos de la Empocaldas S.A. E.S.P. para la entrega de producto, entrega de producto no conforme, pérdida, destrucción o deterioro antes de efectuar la recepción en la Empocaldas S.A. E.S.P..
Esta a cargo del contratista el Incumplimiento de las obligaciones contractuales establecidas, como calidad del elemento suministrado. Fuga de información confidencial y privilegiada de la entidad. Pérdida de los elementos a suministrar.
La forma de mitigarlos será con la constitución de las garantías respectivas, calidad, cumplimiento y responsabilidad civil extracontractual.

SUPERVISIÓN

Nombre del Supervisor	Cargo del supervisor
John Jairo Giraldo Villa	Jefe Secciòn Sistemas

GARANTÍAS

Tipo de garantías	Aplica
Póliza de garantía de seriedad de la oferta.	No aplica
Anticipo	No aplica
Cumplimiento	Sí aplica
Salarios, prestaciones sociales e indemnización de personal	No aplica
Estabilidad y calidad de la obra	No aplica
Responsabilidad civil extracontractual	No aplica
Calidad y correcto funcionamiento de bienes y equipos suministrados	No aplica
Calidad	Sí aplica
Otras: Especificar	No aplica
Otras: Especificar	No aplica
Otras: Especificar	No aplica

TIPO DE CONTRATO

Tipo de contrato	Aplica
Suministros	No aplica
Arrendamiento	No aplica
Obra	No aplica
Prestación de Servicio	Sí aplica
Interventoría	No aplica
Compra Venta	No aplica
Orden de compra	No aplica
Convenio Inter-Administrativo	No aplica
Contrato Inter-Administrativo	No aplica
Otro	No aplica

De acuerdo con lo establecido en el Manual de Contratación de la Empresa y la Ley 142 de 1994, se hace necesario realizar el citado contrato, cumpliendo con los parámetros legales señalados en las normas anteriormente citadas y las demás complementarias. SE CONSIDERA OPORTUNA Y LEGAL LA CELEBRACIÓN DE ESTE CONTRATO

Solicitado por:	
Firma	
Nombre	JOHN JAIRO GIRALDO VILLA
Cargo	Jefe Seccion Sistemas

Aprobado por:	
Firma	
Nombre	MAURICIO ANDRES LOZANO MEJIA
Cargo	JEFE DEPTO ADMINISTRATIVO Y FINANCIERO