AVISO CONVOCATORIA PÚBLICA

SELECCIÓN ABREVIADA DE MENOR CUANTÍA 020 DE 2020

OBJETO: El Instituto para el Desarrollo de Antioquia – IDEA-, está interesado en recibir propuestas para la Selección Abreviada de Menor Cuantía 020 de 2020, cuyo objeto es **PROVEER EL SERVICIO DE UN CENTRO DE OPERACIONES DE SEGURIDAD PARA EL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA-IDEA".**

CLASIFICADOR DE BIENES Y SERVICIOS UNSPSC:
El objeto contractual del presente proceso se encuentra clasificado hasta el tercer nivel dentro de los siguientes códigos del Clasificador de Bienes y Servicios (UNSPSC), así:

Código UNSPSC	Nombre UNSPSC
81141800	Administración de Instalaciones
81111800	Servicios de Sistemas y Administración de Componentes de Sistemas

ALCANCE:

1. Proveer durante 30 meses el servicio de un Centro de Operaciones de Seguridad (SOC) que incluya monitoreos, alertas y gestión de incidentes de forma continua 24x7x365 (24 horas al día, los 7 días de la semana y los 365 días del año) de las siguientes fuentes de la infraestructura critica del Instituto para el Desarrollo de Antioquia:

#	TIPO DE FUENTE O DISPOSITIVO	CANTIDAD
1	Servidor de base de datos	1
2	Aplicación Sistema Financiero	1
3	Firewall (alta disponibilidad activo-pasivo)	2
4	Base de datos	1
5	Servidor Servicios de Directorio	1
6	Servidor Web	1
7	App desarrollo propio para pagos en línea	1
8	Correo electrónico, Almacenamiento y Protección Avanzada de Amenazas en la Nube	180
9	Web Application Firewall	1
10	Switches	2

2. De las anteriores fuentes, se deberán crear como mínimo 3 casos de uso personalizados que hagan referencia a las relaciones entre procesos de negocio, servicios y activos que permite definir lo que se conoce como actores de riesgos o puntos de compromiso. Estos casos de uso podrán ser modificados según la necesidad del IDEA durante la ejecución del contrato.

3. Monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos para un (1) dominio y una (1) marca.

4. Monitorear las fuentes de forma continua (7x24), durante la ejecución del contrato y reportar al IDEA cualquier posible incidente de seguridad que se esté presentando en los dispositivos y/o fuentes críticas a monitorear o que pongan en riesgo su integridad, disponibilidad, autenticidad y confidencialidad.

5. Alertar, atender, clasificar y apoyar activamente la resolución y contención de los incidentes de seguridad del IDEA con detalles completos y acordes con los niveles de servicio requeridos.

6. Generar indicadores de compromiso para cada activo monitoreado, basándose en los ataques recibidos y el uso de amenazas identificadas, así como la detección de uso de aplicaciones o accesos a la plataforma que no concuerden con el patrón histórico de uso o acceso

7. Identificar al menos los siguientes eventos de seguridad mínimos para monitorear:

   - Accesos no autorizados
   - Escalamiento de privilegios.
   - Ataques de fuerza bruta / login.
   - Actividades de cuentas de altos privilegios
   - Usuarios (bloqueados, agregados, eliminados, desbloqueados, cambios de contraseñas)
   - Denegación de servicio.
   - Cambios no autorizados en recursos tecnológicos críticos
   - Explotación de vulnerabilidades.
   - Escaneo de puertos.
   - Detección de brotes de malware.
   - Detección de movimientos laterales.
   - Orígenes de los ataque y principal destino.
   - Ubicación geográfica del ataque.
   - Instalaciones o desinstalaciones de software.
   - Cambios en las políticas del directorio activo.
   -Conexiones (accesos remotos, intentos de conexión)
   -Borrados de logs

8. Prestar el servicio de seguridad que permita al IDEA hacer frente a las amenazas tradicionales y las nuevas amenazas de seguridad (ataques avanzados persistentes, amenazas de día cero, entre otras), así como a las vulnerabilidades detectadas

9. Identificar los riesgos potenciales y amenazas sobre las fuentes criticas definidas, antes de que un ataque real se pueda presentar

10. Dar las recomendaciones técnicas en idioma español, para determinar los controles que permitan mitigar los riesgos en cuanto a la integridad, disponibilidad y confidencialidad, así como en la solución de incidentes de seguridad.

11. La solución de recolección y correlación (SIEM) que utilice el SOC debe ser alimentada por fuentes de inteligencia externas de amenazas que contengan listas de reputación y/o dominios catalogados como sospechosos para la generación de indicadores de compromiso.

12. Implementar un sistema de monitoreo proactivo y centralizado que correlacione eventos de seguridad en línea y fuera de línea de las fuentes entregadas por el IDEA.

13. Realizar monitoreo del comportamiento de tráfico desde y hacia servidores con el fin de detectar actividades inusuales en la infraestructura y realizar análisis comportamental de red y de usuarios.

14. Generar de manera automática las notificaciones de los incidentes al menos a través de estas 3 vías: correo electrónico, llamadas telefónicas y mensajes de texto.

ESPECIFICACIONES TÉCNICAS

1. El SOC deberá tener una arquitectura de seguridad adaptable para lograr combatir el delito cibernético en el panorama de amenazas actual. El equipo SOC debe poder:

   - Prevenir: Este concepto permite adoptar capacidades de identificación y mitigación temprana, para prevenir la materialización de los riesgos que puedan amenazar los activos de información críticos para la organización.
   - Detectar: identificación y mitigación de riesgos que puedan ya estar presentes en el ecosistema corporativo, integrando las tecnologías de seguridad existentes en el ecosistema.
   - Responder: capacidades de prevención y detección, proveer “respuesta continua” y automática a incidentes para la detección y contención de amenazas.
   - Predecir: brindar la atención y primera respuesta de las alertas, integrado metodologías de analítica de datos basadas en indicadores de compromiso (IOC), Business Intelligence (BI) y Redes Neuronales. Es decir, poder predecir ¿cuándo me van a tacar?, ¿cuál es el vector? Y ¿cuáles son los activos que se comprometerán?

2. Las jurisdicciones en donde se procesará las fuentes deben contar con normas equivalentes o superiores a las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos

3. El servicio debe ofrecer un portal web, basado en Business Intelligence (BI) que almacene centralizadamente los reportes, estadísticas y análisis en tiempo real de los eventos capturados; así como la categorización de eventos, incidentes, análisis de riesgo y valoración (alto, medio, bajo). Los supervisores del Contrato por parte del IDEA, deben tener acceso a dicha plataforma.

4. Prestar el servicio de seguridad que permita al IDEA hacer frente a las amenazas tradicionales y las nuevas amenazas de seguridad (ataques avanzados persistentes, amenazas de día cero, entre otras), así como a las vulnerabilidades detectadas

5. Identificar los riesgos potenciales y amenazas sobre las fuentes criticas definidas, antes de que un ataque real se pueda presentar

6. Las soluciones utilizadas deben tener un sólido esquema de datos que permitan agregar la información de todos los dispositivos y/o fuentes entregadas por el IDEA, y correlacionarlos entre ellos (Normalización).

7. Contar con un laboratorio de investigación de nuevas amenazas, así como brindar capacitación técnica constante al personal que lo conforma.

8. El tiempo de retención y almacenamiento de logs y eventos de seguridad debe ser de al menos 30 días en línea y 90 días offline. Estos registros deben almacenarse de manera cifrada por un tiempo mínimo de tres (3) meses para cada dispositivo/sistema y se debe garantizar su disponibilidad para cuando IDEA los requiera.

9. La información propiedad del IDEA que se encuentre en la Nube, debe estar separada y no accesible a otros clientes.

10. El SOC debe tener convenios con entes nacionales e internacionales de los cuales obtenga información o referencias de las últimas técnicas de ciberseguridad, como también, las tendencias en ciberataques a nivel mundial y en el sector. Como mínimo el equipo de respuestas de incidentes debe ser miembro de la Organización Internacional FIRST (Forum for incidents response and security teams) como líder mundial en respuestas a incidentes.

11. En Colombia el SOC debe estar apoyado de organismos como el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), El Centro Cibernético Policial, El Comando Conjunto Cibernético (CCOC), El Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional (CSIRT-PONAL) y El Centro de Coordinación de Atención a Incidentes de Seguridad Informática Colombiano (CSIRT-CCIT).

12. El SOC debe incluir Threat Intelligence o Inteligencia Global, que permite usar un servicio mundial de amenazas identificadas.

13. El SOC debe mantener la tecnología que soporte en un centro de datos principal concurrentemente mantenible: disponibilidad del 99.982%.

14. El SOC debe contar con personal certificado y estar conformado por Un CSIRT (Computer Security Incident Response Team) y/o un CERT (Computer Emergency Response Team) quien deberá responder rápidamente ante un incidente, garantizando la seguridad de la información de forma permanente 7x24x365. el IDEA podrá realizar una o varias visitas al SOC para verificar su estructura.

PRESUPUESTO

Para el presente proceso de selección se tiene un presupuesto oficial estimado en la suma de hasta El presupuesto oficial del presente proceso es de hasta TRECIENTOS NOVENTA Y CUATRO MILLONES SEISCIENTOS CINCUENTA Y DOS MIL NOVECIENTOS CINCUENTA Y NUEVE PESOS M/L ($394.652.959) IVA Incluido, discriminado de la siguiente manera:

VIGENCIA ACTUAL 2020	VIGENCIA ACTUAL 2020	VIGENCIA 2021 11 MESES FEB-DIC	VIGENCIA 2022 12 MESES ENE-DIC	VIGENCIA 2023 6 MESES ENE-JUN	VALOR TOTAL DEL CONTRATO
SERVICIO		$ 149.695.950	$ 163.304.673	$ 81.652.336	$ 394.652.959
AMORTIZACIÓN ANTICIPO		$ 25.982.759	$ 28.344.828	$ 14.172.414	$ 68.500.000
TOTAL A PAGAR	$ 68.500.000	$ 123.713.191	$ 134.959.845	$ 67.479.923	$ 394.652.959

El valor de la vigencia 2020 corresponde al anticipo que se requiere para poner en funcionamiento el SOC

El proponente deberá indicar en la oferta como será invertido el anticipo

El proponente deberá tener en cuenta en su oferta, el pago de impuestos, tasas y otros conceptos que genere su propuesta. Se debe incluir el IVA en el valor total de la oferta, si el proponente no discrimina el IVA, se considerará INCLUIDO en el valor total de la oferta.

APROPIACIÓN PRESUPUESTAL:

Respaldado en el Certificado de Disponibilidad Presupuestal No 202000182 del 21 de abril de 2020. Rubro: 1001000210130 - Servicios Técnicos, expedido por la Dirección de Contabilidad.

Vigencias futuras ordinarias por un valor de:

VIGENCIA 2021	VIGENCIA 2022	VIGENCIA 2023
$ 136.467.084	$ 136.467.084	$ 67.967.084

PLAZO
El plazo de ejecución será de 30 meses a partir de la suscripción del acta de inicio.

LUGAR DE EJECUCIÓN:
En las instalaciones del contratista puesto que allá es donde se encuentran los equipos y el personal especializado para prestar el servicio.

CONSULTA DEL PROYECTO DE PLIEGO DE CONDICIONES
Se podrá consultar el proyecto de Pliego de Condiciones según cronograma. La información relacionada con las reglas de participación en este proceso de selección, así como los estudios y documentos previos pueden ser consultados en el Sistema Electrónico de Contratación Pública (SECOP), link: www.colombiacompra.gov.co.

Durante el término del proceso, la Entidad estatal atenderá a los interesados y recibirá los documentos en desarrollo del proceso de contratación, a través del correo electrónico contratosidea@idea.gov.co.

INVITACION VEEDURÍAS
De conformidad con el inciso tercero del Artículo 66 de la Ley 80 de 1993, el Instituto para el Desarrollo de Antioquia- IDEA- invita a las veedurías ciudadanas para realizar el control social al presente proceso de contratación, para lo cual suministrará la información y documentación requerida, en el Sistema Electrónico de Contratación Pública (SECOP), link: www.colombiacompra.gov.co.

El pliego de condiciones es gratuito, esto es, no tiene ningún valor para el público interesado en presentar propuestas.

LIMITACIÓN A MIPYMES
En el presente proceso de selección no se dará aplicación a lo establecido en el artículo 2.2.1.2.4.2.2 del Decreto 1082 de 2015, respecto a la convocatoria de MIPYMES, toda vez, que realizada la conversión del dólar a moneda Nacional según la tasa cambiaria válida a la fecha de convocatoria del presente proceso de selección, se tiene que el presupuesto oficial corresponde hasta la suma de TRECIENTOS NOVENTA Y CUATRO MILLONES SEISCIENTOS CINCUENTA Y DOS MIL NOVECIENTOS CINCUENTA Y NUEVE PESOS M/L ($394.652.959) IVA Incluido, lo cual se encuentra por encima de los CIENTO VEINTICINCO MIL DOLARES AMERICANOS (US$125,000) equivalente a TRESCIENTOS OCHENTA MILLONES SETECIENTOS SETENTA Y OCHO MIL PESOS ($ 380.778.000), tasa de cambio que para dicho efecto establece el Ministerio de Industria y Comercio con una vigencia del 01 de enero de 2020 hasta el 31 de diciembre de 2021

ENUMERACIÓN Y BREVE DESCRIPCIÓN DE LAS CONDICIONES PARA PARTICIPAR EN EL PRESENTE PROCESO DE CONTRATACIÓN:

1. En el presente proceso de selección podrán participar las personas naturales y jurídicas, nacionales, los consorcios y uniones temporales, promesas de sociedad futura, y demás formas asociativas legalmente constituidas, cuyo objeto social cubra las actividades necesarias para cumplir con el objeto del presente proceso de selección, que no estén reportados en el Boletín de Responsables Fiscales de la Contraloría General de la República, en el SIRI de la Procuraduría General de la Nación, no presentar antecedentes en la Policía Nacional, como tampoco estar vinculado en el sistema Registro Nacional de Medidas Correctiva RNMC de la Policía Nacional de Colombia, además no estar incurso en las prohibiciones, inhabilidades e incompatibilidades consagradas en el ordenamiento legal Colombiano.
2. Los proponentes indicarán si su participación es a título de consorcio o unión temporal, y en el último caso señalarán los términos y la extensión de su participación en la presentación de la propuesta y en la ejecución del contrato, esto es, indicando cuales de las obligaciones contractuales habrán de ejecutar, e indicando el porcentaje de participación en el mismo, de conformidad con lo dispuesto en el parágrafo 1º del artículo 7 de la Ley 80 de 1993, los cuales no podrán ser modificados sin el consentimiento previo del Instituto para el Desarrollo de Antioquia-IDEA-.
3. Los oferentes interesados deben estar inscritos en el Registro Único de Proponentes RUP.
4. Los oferentes interesados deben incluir en su propuesta, la garantía de seriedad, consistente en póliza de seguro, garantía bancaria o patrimonio autónomo.
5. Los oferentes interesados en el presente proceso deben dar cumplimiento a los requerimientos de orden legal, financiero y técnico consagrados en los estudios previos y pliego de condiciones.

CRONOGRAMA DEL PROCESO:

ACTIVIDAD	FECHA Y LUGAR.
Publicación Aviso de Convocatoria Pública.	26 de noviembre de 2020
Publicación de estudios y documentos previos, Proyecto Pliego de Condiciones y borrador minuta del contrato	26 de noviembre de 2020
Plazo para presentar observaciones al Proyecto de Pliego de Condiciones	Hasta el 3 de diciembre de 2020
Publicación Resolución de Apertura y Pliego de Condiciones Definitivo.	04 de diciembre de 2020
Plazo para manifestación de interés por parte de los proponentes	Del 09 al 11 de diciembre de 2020
Publicación del listado de los proponentes que manifestaron interés	14 de diciembre de 2020
Audiencia de Aclaración de pliegos	14 de diciembre de 2020 a las 10:00
Plazo para presentar observaciones al Pliego de Condiciones Definitivo.	14 de diciembre de 2020
Plazo para expedir adendas.	Hasta el 15 de diciembre de 2020
Plazo para presentar propuestas.	Desde el 14 hasta el 17 de diciembre de 2020 a las 10:00 am
Cierre, fecha final de recepción de propuestas.	Hasta el 17 de diciembre de 2020 a las 10:00 am

Apertura de propuestas (Se realizará de forma virtual, para lo cual la Entidad publicará el respectivo aviso con el link para el ingreso de los interesados)	Hasta el 17 de diciembre de 2020 a las 10:15 am
Evaluación de propuestas.	Desde el 17 al 18 de diciembre de 2020
Publicación informe de Evaluación con requisitos a subsanar.	18 de diciembre de 2020
Traslado del Informe de Evaluación y término para subsanar requisitos.	Desde el 21 al 23 de diciembre de 2020
Resolución de adjudicación. Cuando persista el empate entre dos o más propuestas se realizará sorteo mediante el sistema de balotas (de forma virtual, para lo cual la Entidad publicará el respectivo aviso con el link para el ingreso de los interesados)	28 de diciembre de 2020
Expedición del Registro Presupuestal	28 de diciembre de 2020
Celebración del contrato	28 de diciembre de 2020
Publicación del contrato en el SECOP.	Hasta el 29 de diciembre de 2020
Legalización	Hasta el 29 de diciembre de 2020
Ejecución	Ver numeral 6.3 del pliego de condiciones.

FORMA DE PRESENTACIÓN DE LA PROPUESTA

Debido a la situación grave en materia de salud causada por la pandemia del virus COVID-19 y acogiéndonos a medidas tendientes a prevenir los contagios o, por lo menos, a disminuir la velocidad de la propagación del mismo, se utilizarán los medios electrónicos para las entregas de las propuestas de la siguiente manera:

- Las propuestas deben ser remitidas a través del correo electrónico contratosidea@idea.gov.co
- La propuesta debe estar en formato PDF y con contraseña para la apertura de la misma. Si la propuesta viene **sin contraseña, esta no será rechazada, sin embargo, no se podrá garantizar la no apertura de la misma antes de la audiencia de apertura de propuestas**.
- El e-mail no debe pesar en su totalidad más de 20 MB, el proponente debe tener en cuenta que este peso incluye el que puede ir adquiriendo en el trayecto al servidor del IDEA.
- La propuesta debe entregarse en un solo archivo PDF, que tenga un peso máximo de 10 MB con el fin de disminuir el riesgo de sobrepasar el tamaño permitido ya que los encabezados de correo aumentan el tamaño del mensaje. La propuesta, se puede dividir y hacer tantos envíos como sea necesarios, en lo posible no utilizar plataformas en la nube, puesto que el IDEA no se hace responsable por los inconvenientes que se puedan presentar en la descarga de los archivos. El único documento que se envía por aparte de los demás de la propuesta, es el formato de conocimiento del tercero o contraparte, debido a que este puede contener información confidencial del proponente, de manera que si lo presenta en el mismo archivo de la propuesta es bajo su exclusiva responsabilidad.

- La fecha y hora de recibo de las propuestas será la registrada en el correo electrónico contratosidea@idea.gov.co En caso que las propuestas se envíen por partes, no se tendrá en cuenta los correos que lleguen posteriores a la hora de cierre, por lo tanto dichas partes no serán tenidas en cuenta y por tanto no se les dará apertura.
- Tener en cuenta que es responsabilidad del proponente enviarlo con suficiente anterioridad para que el correo llegue antes de la hora de cierre establecida en el cronograma de la invitación numeral 2.1., esto teniendo en cuenta que la hora de envío no será la misma de recibo por parte del correo del IDEA debido a los tiempos de tránsito y validación en los servidores, así como el tráfico de la red. **El Instituto no se hace responsable si por problemas ocasionados en el envío de los correos desde sus cuentas o en la recepción del correo nuestro, la propuesta no puede ser enviada y/o recibida en la hora establecida en el cronograma, por ello se reitera enviarla con suficiente tiempo para poder darle solución a los inconvenientes presentados en forma oportuna**.
- En aras de garantizar a los proponentes que las propuestas no sean abiertas antes de la hora de apertura de las mismas, el proponente deberá enviar el correo con confirmación de recibo y de lectura, dicho correo no será abierto hasta la hora establecida de apertura en el cronograma de la invitación, igualmente deberá enviar al correo contratosidea@idea.gov.co, la contraseña para la apertura del documento en PDF después de la hora de cierre y hasta quince minutos posteriores a la hora fijada para dar inicio a la Audiencia de apertura de propuestas. **Si el proponente no allega la contraseña para dar apertura a la oferta durante este espacio de tiempo, la Entidad no podrá darle apertura a la misma en la Audiencia establecida para tal fin y por lo tanto se entenderá como no presentada la oferta**. Si el proponente presenta la contraseña antes de la hora de cierre, lo hace bajo su exclusiva responsabilidad, toda vez que este es un mecanismo que propende por garantizarle que su propuesta solo sea abierta en el momento indicado. Lo anterior garantizando la transparencia en la recepción y apertura de propuestas y el debido proceso al proponente.
- El correo recibido con la propuesta será radicado en el centro de administración documental por parte de la Dirección Técnica Contractual y Administrativa del IDEA.

No se aceptarán propuestas complementarias o modificaciones que fueran presentadas con posterioridad a la fecha y hora de cierre del presente proceso de contratación.

Las propuestas entregadas en forma extemporánea se entenderán como no presentadas, por lo tanto, no se les dará apertura.

Todos los documentos de la propuesta que tengan modificaciones o enmiendas deben ser validadas con la firma al pie de quien suscribe la carta de presentación, de lo contrario se tendrán por no escritas; no serán tenidos en cuenta para evaluación los documentos que presenten tachaduras o enmendaduras, a menos que tengan la aclaración correspondiente**. Se exceptúa la propuesta económica, la cual, en caso de tener modificaciones, enmiendas o tachaduras, constituirá causal de rechazo**.

Si se presentan ofertas en Consorcio o Unión Temporal u otra forma asociativa permitida por la ley, cada uno de sus integrantes deberá presentar individualmente los documentos que acrediten su capacidad, existencia y representación legal.

La propuesta debe ser presentada en **un (1) original en formato PDF protegido con contraseña, debidamente foliada**, la cual deberá ser entregadas dentro del plazo y hora fijado, y que en el cuerpo del correo se establezca el rótulo, como se señala a continuación:

Señores
INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA-IDEA-
Oficina Gestión del Riesgo
Calle 42 #52-259
Medellín

Selección Abreviada de Menor Cuantía 020 de 2020

Objeto**: "PROVEER EL SERVICIO DE UN CENTRO DE OPERACIONES DE SEGURIDAD PARA EL INSTITUTO PARA EL DESARROLLO DE ANTIOQUIA- IDEA-"**

Sobre: _____
Folios: _____
Datos del proponente
Nombre: _____
Dirección: _____
Teléfono: _____
Fax: _____
Correo Electrónico: _____

La propuesta debe contener un índice o tabla de contenido donde figuren todos los documentos que la componen y el respectivo folio donde se encuentran.

ACUERDO INTERNACIONAL O TRATADO LIBRE DE COMERCIO.
En cumplimiento de lo establecido en el artículo 20 de la Ley 80 de 1993 y en el artículo 2.2.1.2.4.1.3 del Decreto 1082 de 2015, la Entidad realizó la verificación correspondiente estableciendo, de conformidad con el MANUAL PARA EL MANEJO DE LOS ACUERDOS COMERCIALES EN PROCESOS DE CONTRATACIÓN (M-MACPC-06), expedido por Colombia Compra, encontrando la existencia de acuerdo comercial suscrito con El Salvador, y Guatemala.