(+57) 312 630 7973
contacto@bios.co
www.bios.co

Propuesta de colaboración para la construcción de un ecosistema de seguridad digital orientado a la promoción del desarrollo y la generación de capacidades en beneficio de la Nación

Manizales, Octubre 02 de 2023

Señores
COLCERT
MinTIC
Bogotá

Referencia: Propuesta de colaboración para la construcción de un ecosistema de seguridad digital orientado a la promoción del desarrollo y la generación de capacidades en beneficio de la Nación.

Manizales / Caldas / Colombia
Ecoparque los Yarumos

Atendiendo los acercamientos previos con el despacho del señor Ministro, ponemos en consideración la siguiente propuesta de colaboración para desarrollo del plan maestro de capacitación, formación, entrenamiento y sensibilización del recurso humano del país en Ciberseguridad.

Objeto del convenio: Aunar esfuerzos para desarrollar un ecosistema de seguridad digital que impulse procesos de innovación y desarrollo tecnológico, mediante el estudio de escenarios que promuevan la gestión del conocimiento de los riesgos cibernéticos y las afectaciones de los incidentes de seguridad digital entre los diferentes grupos poblacionales del territorio Colombiano - Código TIC 3020001.

En armonía con el objeto, y obedeciendo a la necesidad del Ministerio, BIOS desarrollara los siguiente componentes específicos, entendiendo los mismos como obligaciones especiales del Centro:

1. HUB de Ciberseguridad.

Realizar la estructuración legal, financiera, tecnológica, organizacional de un HUB de Ciberseguridad que fomente la innovación y colabore en la protección de infraestructuras críticas y datos sensibles mediante la prestación de servicios especializados y la formación de talento humano en ciberseguridad.

Entregables:

- ✓ Proyecto para la creación del HUB de Ciberseguridad.
- ✓ Proyecto para la creación del HUB de Ciberseguridad en formato ficha BPIN.
- ✓ Plan de adecuación física y tecnológica de las instalaciones del PTC para albergar al HUB.
- ✓ Informe final de avance en gestiones de presentación y promoción del HUB con diversos aliados potenciales.

Centro de Desarrollo Tecnológico
Technology Development Center
Nit. 900.404.482 - 6

2. Security Operations Center (SOC).

Realizar el diseño técnico, tecnológico, financiero y organizacional de un SOC que preste servicios de seguimiento y monitoreo a entidades públicas y privadas que hacen parte del activo estratégico de la Nación.

Entregables:

- ✓ Informe de diagnóstico y requerimientos técnicos.
- ✓ Propuesta detallada de arquitectura tecnológica.
- ✓ Documento de estructura organizacional y roles del SOC.
- ✓ Plan financiero detallado para la implementación y sostenimiento del SOC.
- ✓ Plan operativo y de gestión del SOC.

3. Plan Maestro de Capacitación, Formación y Entrenamiento en Ciberseguridad.

Plan Maestro para desarrollar debe estar enfocado al desarrollo de las capacidades técnicas del recurso humano del país en los diferentes segmentos definidos, a saber:

Entregables: Los entregables esperados del Convenio son los siguientes:

- ✓ Plan Maestro de Capacitación, Formación y Entrenamiento en Ciberseguridad: Este plan contendrá un análisis de sector y definición de necesidades de recurso humano en ciberseguridad, una definición de segmentos y subsegmentos, una propuesta de estrategia de formación para cada uno y una cuantificación de las metas por segmento para el período 2023-II a 2026-II.
- ✓ Estrategia de comunicación integral para sensibilización ciudadana sobre ciberseguridad para el período 2023-II a 2026-II que defina las audiencias, conocimientos y mensajes clave y que pueda ser ejecutada desde el ministerio en el período definido.
- ✓ Modelo de asociación y alianzas para el logro de alcance del plan maestro: Identificación y gestión de convenios con los aliados potenciales de la industria que están en capacidad y disposición de ofrecer formación pagada, gratuita o subsidiada adicional a la entregada por el ministerio, para alcanzar las metas propuestas. Se deben definir los segmentos a los que estará dirigida esta formación y como se incorporan estos esfuerzos en el plan general.
- ✓ Programa académico formal para formación de Técnico profesional en ciberseguridad: Definición de Syllabus propuesto para el programa, identificación de IES potencialmente capaces de implantar estos programas.

Adicionalmente, y con el fin de cumplir las metas fijadas por MinTic para el periodo 2023-II, se impartirá capacitación a 1800 personas conforme los siguientes segmentos:

Segmento	Meta (Personas)	Mínimo de Horas x Persona
Ciber Líderes	400	20 capacitación /10 horas practicas
Ciber Profesionales	350	20 capacitación /10 horas practicas
Ciber Profesores	50	20 capacitación /10 horas practicas
Ciber Estudiantes	1000	20 capacitación
Total	1.800	Personas formadas

Nota. Dicha capacitación abordará, entre otros, los siguientes ejes temáticos, anotando que los mismos serán depurados en función al interés y objetivos de cada segmento:

- ✓ Seguridad de Redes.
- ✓ Seguridad de Sistemas.
- ✓ Seguridad en Aplicaciones y Desarrollo Seguro.
- ✓ Gestión de Incidentes y Respuesta a Amenazas.
- ✓ Ciber Ranges y Simulaciones.
- ✓ Tendencias y Desafíos Emergentes.
- ✓ Ciberseguridad para Líderes TI.
- ✓ Protección de la Infraestructura TI.
- ✓ Simulaciones de Toma de Decisiones en sala de Crisis.
- ✓ Prácticas de Ciberseguridad Avanzada.
- ✓ Protección de Datos y Privacidad.
- ✓ Simulaciones y Laboratorios Virtuales.
- ✓ Protección en las Redes Sociales.
- ✓ Reconocimiento y Prevención de Amenazas.
- ✓ Seguridad en el Ámbito Laboral e industrial.

Obligaciones especiales del Centro con ocasión del Convenio.

Sin perjuicio de la obligaciones que pueda fijar el Ministerio, BIOS asumirá las siguientes obligaciones en procura del éxito del proyecto:

1. Disponer la capacidad de técnica y humana necesaria materializar el objeto y sus alcance.
2. Presentar el plan operativo necesario para ejecutar el Convenio.
3. Llevar contabilidad independiente para la ejecución del Convenio.
4. Reintegrar mensualmente los rendimientos financieros generados con los recursos girados por el Ministerio en la cuenta que le sea instruida para tal efecto.
5. Celebrar los actos necesarios para la ejecución del Convenio conforme su manual de contratación.
6. Disponer los recursos del convenio para el cumplimiento de las obligaciones derivadas del mismo.

7. Realizar los aportes para la ejecución del Convenio, representados en capacidad técnica y humana.
8. Presentar mensualmente al Supervisor informe de ejecución financiera y cumplimiento de metas.
9. Disponer y hacer uso eficiente de los recursos afectados a la ejecución del Convenio.
10. Designar un representante en el Comité Técnico del Convenio, quien será el encargado del seguimiento técnico, administrativo y financiero durante el término de duración de este.
11. Cumplir con los requisitos establecidos en el Convenio para efectuar los desembolsos.
12. Las demás que sean necesarias e inherentes al objeto del Convenio.

Obligaciones general del Centro con ocasión de la celebración del posible Convenio:

1. Cumplir lo establecido en las políticas de tratamiento de datos personales, seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios y tratamiento de la información de la entidad.
2. Salvaguardar los activos de información del Ministerio/Fondo Único de TIC.
3. Suscribir el documento de compromiso de confidencialidad.
4. Reportar a la mesa de servicio o a quien haga sus veces, los incidentes que afecten o puedan afectar la seguridad y privacidad de la información, seguridad digital y continuidad del servicio de la entidad.
5. Cumplir a cabalidad el objeto en los términos y condiciones aquí pactadas y lo señalado en su propuesta, observando en todo momento la constitución política, las leyes colombianas y el régimen de contratación pública.
6. Ejercer la dirección y el control propio de todas las actividades encomendadas, en forma oportuna y dentro del término establecido, con el fin de obtener la correcta realización del objeto contratado.
7. Responder, sin perjuicio de la respectiva garantía, por el cumplimiento y calidad de los servicios prestados, por el término previsto en el presente contrato.
8. Responder ante terceros por los daños que se ocasionen y que provengan de causas que le sean imputables.
9. Salvaguardar la información confidencial que obtenga o conozca en el desarrollo de sus actividades salvo requerimiento expreso de autoridad competente. Toda la información y/o documentos que se produzcan en desarrollo del presente contrato serán de uso exclusivo del Fondo, obligándose desde ya el contratista a no utilizarlos para fines distintos a los previstos en este contrato, ni a divulgar la información que se le suministre ni los resultados de su trabajo conservando la confidencialidad de los mismos, de conformidad con la Ley, so pena de las acciones civiles, administrativas o penales a que haya lugar.
10. Entregar al supervisor del control de ejecución del contrato, el informe de las actividades realizadas durante el mes o periodo, al igual que los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada cuando así se requiera.
11. Atender los requerimientos, instrucciones y/o recomendaciones que durante el desarrollo del contrato le imparta el Fondo a través del supervisor del mismo, para una correcta ejecución y cumplimiento de sus obligaciones.
12. Reportar, de manera inmediata al supervisor, la ocurrencia de cualquier novedad o anomalía durante la ejecución del contrato.
13. Informar sobre peticiones o amenazas de que sea objeto por quienes actúen por fuera de la ley, con el propósito de obligarlo a hacer o a omitir algún acto o hecho, al Fondo a través del funcionario responsable de la supervisión y control de ejecución, y a las demás autoridades competentes para que se adopten las medidas y correctivos que fueren necesarios.
14. Responder por la pérdida total y/o parcial de los documentos que obren en los expedientes contractuales que por motivo de sus obligaciones contractuales deba custodiar y/o manipular y/o emplear.
15. Presentar la factura electrónica previamente validada por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, conforme con las disposiciones señaladas en el Decreto 358 de 2020, en concordancia con lo dispuesto en la Resolución No. 000042 de 2020, en los casos que aplique.

Valor del proyecto: El valor del estimado para el desarrollo del proyecto será hasta de *cinco mil cien millones de pesos* ($5.100’000.000) incluido IVA, costos y gastos financieros y tributarios a que hubiere lugar, distribuidos así:

- ✓ El Ministerio aportará *cuatro mil ochocientos millones de pesos* ($4.800’000.000).
- ✓ BIOS aportara *trescientos millones de pesos* ($300’000.000).

La distribución de recursos obedece al siguiente nivel de detalle:

Aportes del Ministerio para desarrollo de Convenio y la materialización de la metas: Cuatro mil ochocientos millones de pesos ($4.800’000.000), desembolsados conforme los siguientes flujos de recursos en armonía con los entregables que implica la ejecución del propuesto:

Concepto	Entregable	%	Valor
Primer desembolso Nov/17/2023	a. Diseño plan de trabajo. b. Cronograma de actividades. c. Diseño metodología de desarrollo del proyecto. **Nota.** El 21 de noviembre se entregaría el Plan de trabajo, el Cronograma definitivo de actividades y la Metodología de desarrollo del proyecto consolidados.	31%	$1.500.000.000
Segundo desembolso Nov/24/2023	a. Diseño de la estrategia de comunicación ciudadana sobre ciberseguridad. b. Diseño del modelo de alianzas para el logro de las metas de formación en ciberseguridad. c. Diseño de un programa de educación formal en técnico en ciberseguridad que pueda ser implantado en diversas instituciones de educación superior. d. Estructuración técnica, legal, financiera y organizacional del Hub de Ciberseguridad. e. Diagnóstico y definición de requerimientos técnicos específicos para el SOC. f. Diseño arquitectura tecnológica para el SOC. **Nota.** El 30 de noviembre se entregaría la Estrategia de comunicación ciudadana, el Modelo de alianzas para logro de las metas de formación en ciberseguridad, el Programa de educación formal técnico, la Estructuración técnica, legal, financiera y organizacional del Hub, el Diagnóstico y definición de requerimientos técnicos para el SOC, y la Arquitectura tecnológica para el SOC consolidados.	48%	$2.300.000.000
Tercer desembolso Dic/15/2023	a. Desarrollo ciclo de formación mediante la capacitación de 1800 personas en ciberseguridad de acuerdo con las metas definidas en cada segmento definido en el anexo técnico. b. Informe de identificación y documentación de requisitos para la implementación del HUB en el Parque tecnológico de Villamaría en los componentes físicos y tecnológicos, incluyendo presupuesto estimado para las adecuaciones. c. Informe de identificación de Aliados Potenciales. d. Informe de establecimiento de espacios para realizar ruedas de negocios y definir contactos con empresas e instituciones que estén interesadas en participar en el HUB, en los distintos roles definidos. e. Estructura organizacional y roles del SOC. f. Plan financiero implementación y sostenimiento del SOC. g. Plan operativo y de gestión del SOC. **Nota.** El 15 de diciembre se entregaría el Informe desarrollo del ciclo de formación, Informe de identificación y documentación de requisitos para la implementación del HUB en el Parque Tecnológico de Villamaría, el Informe de identificación de Aliados Potenciales, el Informe de establecimiento de espacios para ruedas de negocios y contactos institucionales con interesados en participar en el HUB, en Estructura organizacional y roles del SOC, el Plan financiero para implementación y sostenimiento del SOC, y el Plan operativo y de gestión del SOC.	21%	$1.000.000.000
Total			**$4.800.000.000**

Aportes de BIOS para desarrollo de Convenio y la materialización de la metas: Trecientos millones de pesos ($300’000.000) en especie, así:

- ✓ Logos y manual de imagen del Hub de Ciberseguridad: $50’000.000.
- ✓ Desarrollo de 10 cortos y/o videos animados sobre Ciberseguridad dirigidos a los ciudadanos, con logos e imagen institucional del Ministerio: $250’000.000.

Nota. Conforme su naturaleza jurídica, el Convenio propuesto resultara de medio y no de resultado, y por lo tanto podrá haber desistimientos de los cursos por parte de quienes en ellos se matricularon, sin que ello sea por causa del Aliado, pudiendo existir un margen de hasta el 10% de matriculados no graduados, sin que ello resulte en una disminución del valor pagado al Aliado, por cuanto los cursos causan gastos en su creación y prestación, aunque el alumno no termine exitosamente el mismo.

Validez jurídica del Convenio: Conforme el numeral 1 del artículo 2 de la Ley 1150 de 2007, que trata de las modalidades de selección, la escogencia del contratista se efectuará por regla general a través de licitación pública, con las excepciones que se señalan en los numerales 2, 3 y 4 del artículo ibidem, entendiendo por licitación el procedimiento mediante el cual la entidad estatal formula públicamente una convocatoria para que, en igualdad de oportunidades, los interesados presenten sus ofertas y seleccione entre ellas la más favorable según la definición del parágrafo único del artículo 30 de Ley 80 de 1993. Sin perjuicio de lo anterior, resulta valido precisar que, además del Estatuto General de la Contratación de Administración Pública, nuestro sistema normativo de fuentes comparta la existencia de disposiciones especiales en materia de contratación, y entre estas, el Decreto 393 de 1991 *“Por el cual se dictan normas sobre asociación para actividades científicas y tecnológicas, proyectos de investigación y creación de tecnologías”*, según el cual resulta posible a la administración pública adelantar actividades científicas y tecnológicas, al igual que impulsar proyectos de investigación y de creación de tecnologías, a treves de la asociación con particulares bajo dos modalidades: 1. Creación y organización de sociedades civiles y comerciales y personas jurídicas sin ánimo de lucro como corporaciones y fundaciones, y 2. Mediante la celebración de convenios especiales de cooperación, precisando que la celebración de los convenio especial de cooperación de los que trata el numeral 2 del artículo 1 del decreto ibidem, resulta válida para *“Formar y capacitar recursos humanos para el avance y la gestión de la ciencia y la tecnología”* conforme el literal d del artículo 2 del mismo decreto.

Dicho lo anterior, resulta oportuno y conveniente señalar que BIOS, como Aliando del Ministerio para la ejecución del Plan propuesta, surgió como una iniciativa de la Nación (representada por MinTIC y Colciencias, hoy MinCiencias), la empresa privada (representada por Microsoft y Hewlett Packard), y la academia (representada por la Universidad Nacional de Colombia, Universidad de Caldas, Universidad Tecnológica de Pereira, Universidad del Quindío y el Sistema Universitario del Eje Cafetero) para fortalecer la investigación y los servicios de computación de alto rendimiento, antecedente que justifica la modalidad de selección.

Idoneidad y capacidad de BIOS para el desarrollo del Convenio: BIOS está equipado con tecnología de vanguardia, incluyendo potentes sistemas informáticos, redes de alta velocidad y acceso a recursos especializados en ciberseguridad. Estas capacidades permiten realizar simulaciones complejas y tareas intensivas que son fundamentales para la capacitación en la materia objeto del Convenio.

Desde dicha óptica, ostentar la titularidad de supercomputadores le permite abordar problemas complejos de ciberseguridad mediante el uso de técnicas de paralelismo, lo que acelera el tiempo de entrenamiento y análisis de datos, condición especialmente útil cuando se trata de grandes cantidades de datos y análisis de malware. Dado lo anterior, BIOS puede simular entornos de red y sistemas informáticos reales para que los estudiantes practiquen sus habilidades en escenarios más cercanos a situaciones del mundo real, elementos objetivos que contribuyen a mejorar la preparación para enfrentar amenazas reales y desarrollar habilidades prácticas.

Adicionalmente, BIOS es un reconocido actor del ecosistema de ciencia y tecnología de la nación, capaz de articular actores públicos y privados para la gestión de conocimiento y el impulso de procesos de capacitación de alto impacto, contando dentro sus aliados estratégicos para la formación científica del recurso humano, con la Universidad Nacional de Colombia, la Universidad de Caldas, y la Universidad Tecnológica de Pereira, y adicionalmente, con el apoyo de Microsoft e IBM como actores lideres del

mercado para la provisión de herramientas de hardware y software para ciberseguridad, factores diferenciadores que confieren al Centro la capacidad suficiente para satisfacer la necesidad del Ministerio. Desde esta óptica, BIOS posee además otras potencialidades:

- ✓ **Especialidad, unicidad y vínculo especial con MinTic:** BIOS es una entidad única en Colombia que combina una amplia gama de especialidades, incluyendo bioinformática, ciencia de datos, ciberseguridad, computación de alto rendimiento (HPC) e infraestructura tecnológica. Su misión, centrada en la generación de valor a través de la incorporación efectiva de tecnologías avanzadas en el ecosistema de tecnología del país, hace que BIOS sea un actor fundamental en el sector tecnológico y de ciberseguridad de Colombia. Aquí cabe resaltar que BIOS fue creada por iniciativa de la Nación como corporación sin ánimo de lucro de carácter privado, contando con participación de MinTic en su junta directiva, sido además el principal aportante desde su creación.
- ✓ **Liderazgo en Ciberseguridad:** BIOS es el líder promotor del HUB de Ciberseguridad (que será ubicado en Villamaría) en concurso con la Gobernación del Departamento de Caldas, contando para tal efecto con alianzas y acuerdos vigentes con los principales actores de la ciberseguridad nacional del Estado colombiano y con las principales empresas tecnológicas nacionales y multinacionales del sector, las cuales se encuentran interesadas en ofrecer coordinadamente sus productos y servicios a través del HUB para fortalecer las capacidades técnicas y humanas del país en materia de ciberseguridad.
- ✓ **Recurso Humano:** El talento humano de BIOS es uno de sus mayores activos, contando con ingenieros, programadores, expertos en ciencia de datos, y expertos en ciberseguridad, tanto en su equipo técnico, como provenientes de las universidades públicas del Eje Cafetero que concurren al Centro. En el ámbito de la ciberseguridad se considera fundamental un conocimiento amplio y agnóstico de las diversas tecnologías disponibles en el mercado, para lo cual BIOS tiene establecidas diversas alianzas en formación con los líderes de ciberseguridad del mercado tecnológico.
- ✓ **Experiencia:** BIOS ha demostrado su experiencia y capacidad para manejar proyectos de gran envergadura en el ámbito de la ciberseguridad, la bioinformática, la ciencia de datos y las tecnologías avanzadas. Sus proyectos en formación incluyen la creación de aulas virtuales para ofrecer cursos avanzados de tecnología propios y de las universidades vinculadas, la capacitación de empresarios en tecnología y la formación avanzada de investigadores en diversas tecnologías avanzadas. Así mismo ha sido ejecutor habitual y cumplido de los diversos proyectos estratégicos de MinTic desde el año 2011 al igual que proyectos de regalías de ciencia y tecnología.
- ✓ **Relacionamiento e infraestructura.** BIOS está equipado con tecnología de vanguardia, incluyendo potentes sistemas informáticos, redes de alta velocidad y acceso a recursos especializados en materia de ciberseguridad al amparo de acuerdos con actores de mercado reconocidos tales como IBM, Bulkware, Td Synnex y Lenovo, entre otros, relacionamiento que le permitiría estructurara simulaciones complejas y tareas intensivas de apropiación de conocimiento que resultan fundamentales para la formación en la materia.

Termino de duración: Desde la suscripción del acta de inicio y hasta el 31 de diciembre de 2023.

Paula Marcela Arias Pulgarín
Directora Ejecutiva
paula.arias@bios.co

Aviso de confidencialidad: Este documento es de carácter confidencial, reservado y están protegidos por las leyes de derechos de autor. El contenido va dirigido, de manera exclusiva, a su destinatario y contiene información confidencial y sujeta a la protección de secreto empresarial, y su divulgación no está permitida por la ley. En caso de recibir este documento por error, le solicitamos nos lo comunique inmediatamente a través de nuestro equipo de soporte: contacto@bios.co y proceda a su eliminación, así como a la de cualquier documento anexo al mismo. Le comunicamos que si usted no es el destinatario original, la distribución, copia o utilización de este documento o de sus anexos, cualquiera que sea su finalidad, están prohibidas por la ley.