

CENTRO DE BIOINFORMÁTICA
Y BIOLOGÍA COMPUTACIONAL

Conocimiento e innovación para el desarrollo

Propuesta:

“Proyecto de retos de innovación tecnológica en ciberseguridad”

Objeto: Aunar esfuerzos técnicos, administrativos y financieros para implementar una estrategia basada en la transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información

Septiembre de 2024

1. AVISO DE CONFIDENCIALIDAD

Los destinatarios y receptores de la presente propuesta, reconocen y aceptan que toda la información presentada, metodologías, modelos, Know How, el plan técnico y su desarrollo, la descripción del trabajo a realizar, la información sobre las hojas de vida de los investigadores, y la propuesta financiera sobre el costo del desarrollo del proyecto, tienen el carácter de confidencial, y por lo tanto la empresa, compañía, entidad, o institución receptora; así como todas y cada una de las personas que detente la calidad de subordinados, empleados o dependientes y que tengan acceso a la información con ocasión de la presente propuesta; se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros, todas las informaciones y datos suministrados en la misma. La Cláusula de confidencialidad se regirá por la reglamentación sobre Informaciones Confidenciales y Secretos Industriales de que tratan los artículos 260 a 266 de la Decisión 486 de la Comisión del Acuerdo de Cartagena.

PROPIEDAD INTELECTUAL SOBRE LOS CONTENIDOS: Los destinatarios y receptores de la presente propuesta, reconocen y aceptan que el contenido de la misma contiene material, productos o procedimientos, contenidos e información protegida por las normas nacionales y extranjeras vigentes sobre Propiedad Intelectual. Por lo tanto cualquier utilización, reproducción, comunicación pública, transformación, distribución, alquiler, préstamo público e importación, total o parcial, en todo o en parte, en formato impreso o digital se encuentran prohibidos, y sólo serán lícitos en la medida en que se cuente con la autorización previa y expresa por escrito del Centro de Bioinformática y Biología Computacional. Todo lo anterior de conformidad con lo establecido en la normatividad vigente en Propiedad Intelectual, particularmente con lo establecido en el Convenio de Berna, el Convenio de París; la ley 23 de 1982, Ley 44 de 1993, ley 1450 de 2011, la Decisión Andina 351 de 1993, La Decisión Andina 345 de 1993, la Decisión Andina 486 de 2000, y en general los convenios internacionales sobre la materia de los cuales Colombia es miembro; y demás normas concordantes que las modifiquen o adicionen.

Tabla de contenido

1. AVISO DE CONFIDENCIALIDAD.....3
Tabla de contenido.....5
2. JUSTIFICACIÓN.....6
2.1. MERCADO DE LA CIBERSEGURIDAD EN EL MUNDO.....6
2.2. ESTADO DE LA CIBERSEGURIDAD EN COLOMBIA.....7
2.3. LA INDUSTRIA DE LA CIBERSEGURIDAD EN COLOMBIA.....10
2.4. EMPRESAS DE CIBERSEGURIDAD EN COLOMBIA.....14
3. GENERALIDADES.....16
3.1. OBJETIVOS.....16
3.2. ALCANCE (Componentes y Entregables del Proyecto).....17
4. TRAYECTORIA DE BIOS.....19
5. EQUIPO DE TRABAJO.....21
6. PRESUPUESTO ESTIMADO.....22
7. SEGURIDAD DE LA INFORMACIÓN.....26
Cumplimiento de la Política de Seguridad MinTIC.....26
Políticas de Borrado Seguro.....26
Formatos y documentos.....27
8. CUMPLIMIENTO LEY 1581 DEL 2012.....27

2. JUSTIFICACIÓN

2.1. MERCADO DE LA CIBERSEGURIDAD EN EL MUNDO

Según análisis especializados en la materia:

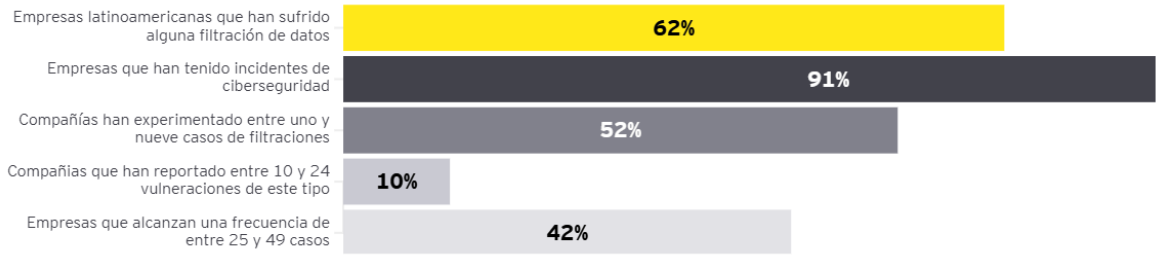
"El tamaño del mercado de ciberseguridad (en el mundo) se estima en USD 182.86 mil millones en 2023, y se espera que alcance los USD 314.28 mil millones para 2028, creciendo a una tasa compuesta anual de 11.44% durante el período de pronóstico (2023-2029)" (En: https://www.mordorintelligence.com/es/industry-reports/cyber-security-market).

El gasto mundial en productos y servicios de ciberseguridad va a crecer un 13,2% en 2023, según las previsiones de la consultora Canalys (En: https://www.canalys.com/newsroom/cybersecurity-forecast-2023). La cifra total de inversión de las empresas podría llegar hasta los 223.800 millones de dólares. La misma organización prevé que el gasto mundial en ciberseguridad aumentará un 13,2% durante este año, y se elevará a 223.800 millones de dólares en el mejor de los escenarios previstos cuyos expertos destacan que el crecimiento que se producirá en la categoría de servicios (Ibidem).

"Se prevé que la prestación de servicios de ciberseguridad, categoría que incluye, externalización, consultoría, despliegue, integración, mantenimiento y seguridad gestionada, crezca un 14,1% hasta los 144.300 millones de dólares en 2023. Esto representará el 64,5% del mercado mundial de ciberseguridad en 2023" (En: https://protecdatalatam.com/noticias/las-empresas-aumentaran-el-gasto-en-ciberseguridad-mas-de-un-13-en-2023/Protecdata).

Las ventas de productos de ciberseguridad, que incluye la seguridad de endpoints, la seguridad de red, la seguridad web y del correo electrónico, la seguridad de los datos, la gestión de identidades y accesos, y el análisis de vulnerabilidades y seguridad, registrarán un aumento del 11,7%, hasta los 79.500 millones de dólares en 2023. Esto representa un crecimiento robusto para el sector tecnológico, pero también es una desaceleración de los niveles de 2022, cuando las organizaciones aumentaron el gasto para actualizar las defensas existentes y agregaron nuevas capacidades, especialmente en la nube, IoT/OT y seguridad de identidades (En: https://www.ituser.es/seguridad/2023/01/las-empresas-aumentaran-el-gasto-en-ciberseguridad-mas-de-un-13-en-2023).

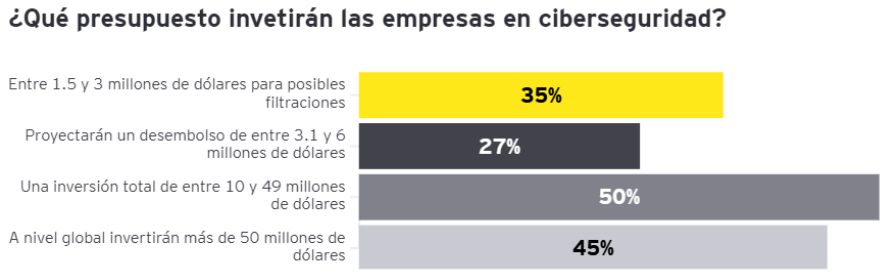
El estudio EY 2023 Global Cybersecurity Leadership Insights reseña que el "62% de las empresas latinoamericanas han sufrido alguna filtración de datos durante el último año. Por su parte 52% de las compañías latinoamericanas han experimentado entre uno y nueve casos de filtraciones. Igualmente 50% de las empresas de Latinoamérica reportaron una inversión total en ciberseguridad de entre 10 y 49 millones de dólares" (En: www.ey.com/es_co/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy).



Fuente: EY Global Cybersecurity Leadership Insights Study, 2023.

El precio de los ataques

"A nivel de costos, durante 2022 un 37% de las empresas señaló que las filtraciones sumaron un gasto de menos de 1.5 millones de dólares; y un 35% comentó que este valor alcanzó entre 1.5 y 3 millones de dólares" (Ibidem). Según la misma fuente en cita, la Inversión planeada para 2023 es:



"De hecho, según el Índice Global de Ciberseguridad más reciente, elaborado por la International Telecommunication Union de Naciones Unidas, Latinoamérica es la región del mundo más vulnerable a los ataques cibernéticos y presenta el índice más bajo de preparación contra este tipo de delitos" (El Tiempo, edición de 23 de septiembre 2023).

2.2. ESTADO DE LA CIBERSEGURIDAD EN COLOMBIA

En el año 2021 se presentaron más de 7 billones de intentos de ataques cibernéticos en nuestro país según la Cámara Colombiana de Informática y Telecomunicaciones (En: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/).
En el mismo sentido, la Fiscalía General de la Nación reportó un aumento del 30% en el número de dichos ataques (Ibidem). Casos recientes como los ataques sufridos por Keralty o IFX Networks, que prestan servicios a diferentes entidades de gobierno, o los eventos sufridos por el Ministerio de Salud y Protección Social o el Consejo Superior de la Judicatura, demuestra la susceptibilidad de Colombia (En: https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/).

Se reportaron 54.121 denuncias por ciberataques en el país durante el año 2022, esto según estadísticas del Centro Cibernético de la Policía Nacional, lo que representa un incremento del 79% frente al año anterior. "Este panorama hace que sea urgente la colaboración entre las agencias gubernamentales y las compañías de ciberseguridad para compartir información sobre las amenazas, desarrollar estrategias de mitigación y apoyar a las víctimas de estos ataques. Desafortunadamente, estas iniciativas aún son "muy incipientes" (Forbes Colombia, edición de octubre 9 de 2023).

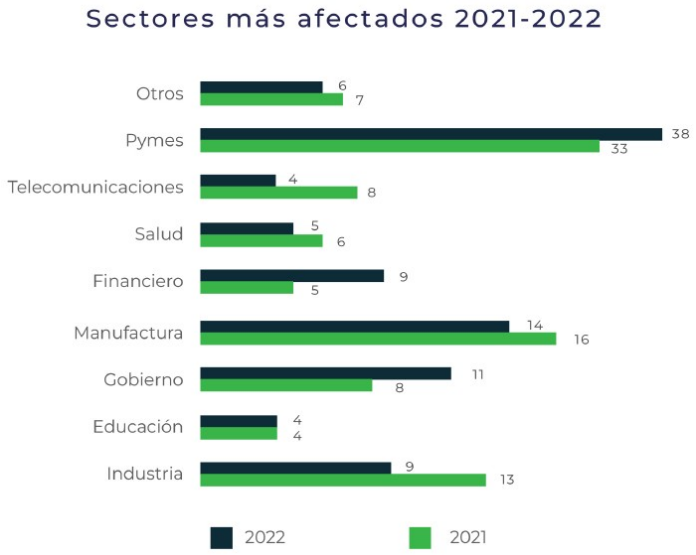
Colombia específicamente ha enfrentado al menos dos grandes ataques cibernéticos en menos de un año, capaces de poner en jaque al país entero. El primero ocurrió en noviembre de 2022, cuando el Grupo Keralty sufrió un robo de datos clasificados por parte del grupo de hackers Ransomhouse, que publicó la mitad de la información al no ver satisfechas sus pretensiones económicas. El segundo tuvo lugar a mediados de septiembre, cuando la empresa de telecomunicaciones IFX Networks fue víctima de un ataque que afectó a más de 760 entidades públicas y privadas, entre ellas varias proveedoras estatales de servicios digitales (Ibidem).

En el mismo marco, y conforme los análisis y registros de la Cámara Colombiana de Informática y Telecomunicaciones, las ciudades en Colombia con mayor afectación de ataques cibernéticos son:



Fuente: Informe Anual de Ciberseguridad, Cámara Colombiana de Informática y Telecomunicaciones, 2023 (disponible en https://www.ccit.org.co/estudiosobs/).

Por su parte los sectores económicos más afectados son:



Fuente: Ibidem.

Cabe señalar que durante el año 2023, se registraron más de 5.000 millones de intentos de ciberataque en Colombia, lo que la sitúa como la cuarta nación más afectada en América Latina, después de Brasil, México y Venezuela según datos de Fortinet (Cfr. https://canal1.com.co/noticias/empresas/ciberseguridad-colombia-plataforma-detecta-ciberataques/). De acuerdo con el Global Digital Trust Insights 2023 de PwC Colombia "menos del 40% de los líderes en Colombia ha mitigado por completo los riesgos de ciberseguridad emergentes" (Cfr. https://lanotaeconomica.com.co/movidas-empresarial/tendencias-y-retos-para-este-2023-en-ciberseguridad-en-colombia/). Adicionalmente, según análisis de PwC Colombia, "(…) los altos ejecutivos se preocupan porque su empresa no esté totalmente preparada para hacer frente a las mayores amenazas. Según los encuestados en Colombia, las principales amenazas que pueden afectar en mayor medida a sus empresas, en el año 2023, serán perpetradas principalmente por Ciberdelincuentes

(65%), Hackers (51%) y Amenazas internas (44%)" (Ibidem). Siguiendo esta línea, fuentes autorizadas en la materia sostienen que:
Una de las grandes debilidades que ha generado importantes impactos en las organizaciones en Colombia es la falta de una estrategia y una arquitectura de seguridad robusta, que identifique y mitigue continuamente los diferentes riesgos a los que está expuesta la entidad y cuente con un presupuesto para ello. A pesar de que los ciberataques pueden costar millones de dólares a las organizaciones aún no existe claridad frente al nivel de exposición a estos riesgos e iniciativas concretas para mitigarlos. Es importante incluir la ciberseguridad en cada actividad de negocio, como un proceso continuo, para así mitigar de forma preventiva los riesgos asociados.

Entre los riesgos más comunes que se esperan para este año y en los que más deben estar centradas las organizaciones estarían a la orden del día temas relacionados con Hackeo y fuga de la información, la explotación de servicios de componentes en la nube y ataques de ransomware. Adicionalmente, se evidenció que entre las principales vías por las cuales se vulnera la seguridad en las empresas en Colombia estarían los celulares, el correo electrónico, infraestructura en la nube y aplicaciones web, mostrando que menos del 50% de las empresas cumplen con todas las habilidades requeridas para la divulgación externa de estos tópicos (En: https://unipymes.com/tendencias-y-retos-para-este-2023-en-ciberseguridad-en-colombia/).

Muestra de lo anterior, la Asociación Bancaria y de Entidades Financieras de Colombia - Asobancaria, reporta que actualmente se registran alrededor de 43 ciberataques por segundo al sistema financiero colombiano. Se trata de un riesgo de grandes proporciones, considerando que hoy en día un 68% de todas las transacciones monetarias del país se realizan a través de canales digitales y servicios de banca en línea (Cfr: https://lanotaeconomica.com.co/movidas-empresarial/el-34-de-las-empresas-en-colombia-han-sufrido-algun-tipo-de-fraude-en-plataformas-digitales/). A su vez, la Superintendencia Financiera señaló que tan solo en año 2021 los bancos del país recibieron un total de 1.362 millones de ataques, que resultaron en un costo de 75.000 millones de pesos en reposiciones e indemnizaciones por operaciones no autorizadas. Para mitigar estos riesgos, el sector financiero colombiano ha aumentado en un 141% la inversión en sistemas de ciberseguridad, que hoy asciende a un monto cercano a los 400 mil millones de pesos al año (Ibidem).

No obstante, cabe decir que los esfuerzos por mejorar la seguridad de la banca digital han rendido sus frutos. Asobancaria estima que en la actualidad, el 99% de las operaciones financieras a través de canales digitales en el país se realizan de manera segura. Por cada 100 dólares de transacciones dentro del sistema bancario, solo 1 tiene reclamación por fraude de parte de los clientes, una estadística muy positiva que refleja la fortaleza de los sistemas de seguridad de la banca nacional. En Colombia, el 34% de las empresas reportan haber experimentado algún tipo de fraude en sus plataformas digitales en los últimos dos años. El 94% de las empresas aseguran estar conscientes de riesgos de fraude, pero solo un 76% monitorea proactivamente sus plataformas. Un 80% considera que cuentan con controles suficientes para detectar fraudes en línea, incluyendo tecnologías de monitorización de transacciones y detección de anomalías en los registros de operaciones financieras (Ibidem).

El Informe 2023 Attack Surface Threats de Unit 42, de la unidad de investigación e inteligencia de amenazas de Palo Alto Networks señala que *"Colombia sigue en la mira: 85% de las empresas con trabajo remoto son vulnerables a ataques de ransomware. En Colombia el ciberdelito aumentó un 26% en 2022 en comparación con el año anterior y el 67% de las denuncias de ciberataques se registran por empresas públicas y privadas. Además, el país sigue en la mira de los ciberdelincuentes, no en vano fue víctima*

recientemente de un ataque de ransomware a gran escala" (En: https://www.infobae.com/inhouse/2023/10/18/colombia-sigue-en-la-mira-85-de-las-empresas-con-trabajo-remoto-son-vulnerables-a-ataques-de-ransomware/Infobae, 2023). Así las cosas, resulta lugar común afirmar que los principales problemas de ciberseguridad, tanto en Colombia como los demás países de la región, están dados por el phishing, el whaling, el malware o software malicioso y las descargas automáticas, eventos que sin duda han acelerado la inversión en ciberseguridad en todos los sectores de la economía. Según análisis realizados por Boston Consulting Group, *"la inversión en ciberseguridad crecerá a un ritmo de aproximadamente el 8% en Latinoamérica hasta 2024"* (En: https://www.bcg.com/press/13may2021-pandemic-accelerated-investment-in-cybersecurity-by-colombian-companies).

En términos de análisis económico, Soto y Cifuentes sostienen que el sector TIC en Colombia registra un producto promedio cercano a $20 Billones de pesos, teniendo en cuenta que en 2018 alcanzó $19,55 billones, creciendo a $20,3 Billones en 2019 y logrando $20,1 billones para 2020, registrando una contracción de apenas el -1%, en comparación con otros sectores económicos que registraron caídas superiores al 10% producto de la pandemia del covid-19. Dicho comportamiento es explicado, entre otros factores, por la adopción del teletrabajo que obligó a las empresas a actualizar y mejorar sus esquemas de ciberseguridad, donde sus trabajadores empezaron a realizar sus funciones desde casa o en sus propios dispositivos, exponiendo las redes de datos de las empresas, ya que es muy poco común que los individuos tuvieran ya instalados sistemas de ciberseguridad para sus hogares. Así mismo, se considera que Colombia es el segundo país más afectado por ataques cibernéticos en la región latinoamericana, después de Brasil, con 1,8 millones de intentos, indicando la necesidad de fortalecer esquemas de ciberseguridad nacionales. Cada día los datos cobran mayor valor, por lo cual es de suma importancia protegerse frente a ataques cibernéticos. En Colombia, entidades cómo la Asociación Nacional de Industriales demuestran que el 50% de las empresas ha sido afectada por algún tipo de ciberataque, por lo cual se sugieren que la inversión en ciberseguridad no sea vista por las empresas cómo un gasto, sino una inversión (Cfr. https://repository.javeriana.edu.co/bitstream/handle/10554/64394/Propuesta%20comercial%20para%20aumentar%20los%20ingresos%20de%20las%20cuentas%20de%20Trellix%20Colombia%20con%20facturación%20menor%20a%20USD%20%241.000.pdf?sequence=5&isAllowed=y).

En respuesta a tales eventos, el gobierno ha emprendido acciones de fortalecimiento de políticas públicas a través de la expedición de documentos CONPES y la creación de instrumentos policiales y judiciales para enfrentar amenazas de ciberseguridad. Para tal efecto, y según los análisis del portal especializado Bloomberg con fundamento en datos suministrados por MinTic, la inversión total del estado colombiano en los últimos años para atacar este fenómeno ilegal has sido de cerca $109.000 millones de pesos, cifra baja si se la compara tan solo con la inversión realizada por España, superior a los 120 millones de Euros (Cfr.: https://www.bloomberglinea.com/2023/01/13/en-que-ha-gastado-colombia-los-109000-millones-que-invirtio-en-ciberseguridad-desde-2011/).

2.3. LA INDUSTRIA DE LA CIBERSEGURIDAD EN COLOMBIA

Según la organización Informes de Expertos, el tamaño del mercado de la ciberseguridad en Colombia alcanzó un valor de 243,86 millones de dólares en 2022. Además, durante el período de pronóstico de 2023-2028, se anticipa que el mercado refuerce a una CAGR del 14,70%. Este contempla posibilidades relevantes de crecimiento para alcanzar un valor cercano a los 555,29 millones de dólares en 2032. Sin embargo, el mercado objetivo ha llevado a cabo todos los registros de las empresas que han sufrido hasta un 44% de ataques de ransomeware en Colombia y México en 2020 y sus políticas de seguridad para

asignar soluciones de ciberseguridad con intención de prevenir infecciones de malware en los sistemas. A su vez, la política de desarrollo de la estrategia nacional de ciberseguridad de Colombia ha dado como resultado obtener la puntuación más alta de 5 rangos bajo el Modelo de Madurez de Capacidades (CMM) en 2020. Por otra parte, la demanda de ciberseguridad mostró un aumento del 40% en Colombia en 2020, según informó la Cámara Colombiana de Informática y Telecomunicaciones. Estas prospecciones están perfilando las perspectivas del mercado de la ciberseguridad en Colombia con importantes inversiones y medidas drásticas del gobierno local (En: https://www.informesdeexpertos.com/informes/mercado-de-la-ciberseguridad-en-colombia).

Siguiendo con fuente Ibidem, los factores clave que determinan las perspectivas del mercado colombiano de la ciberseguridad son:

- Adopción de la digitalización para el entorno de trabajo por diversos sectores industriales.

  La creciente adopción de espacios de trabajo basados en la nube híbrida por parte de los sectores BFSI, TI y telecomunicaciones, sanidad y otros se traduce en una gran amenaza para la información crítica y sensible almacenada en la nube. Este cambio digital ha llevado a la expansión del mercado debido a la creciente demanda de seguridad de tecnologías de información y datos, redes, nube y otras sistemas. Por lo tanto, cuanto mayor sea el uso de Internet, mayores serán los riesgos para los datos y los ciberataques, lo que contribuirá a ampliar de la cuota de mercado de ciberseguridad en Colombia

- Integración de nuevas tecnologías y activos electrónicos, una amenaza para el mercado objetivo.

  La apuesta consolidada de la tecnología en cada etapa de la vida, ya sean oficinas, escuelas o casas, la tecnología está en todas partes, en todos los aparatos y lugares, lo que ha supuesto una amenaza para la ciberseguridad. Además, el alto consumo de Internet de las cosas (IoT), el aprendizaje automático, la inteligencia artificial (AI) está detectando las amenazas inciertas de los ciberataques. Con la preponderancia de los delitos cibernéticos, se requiere la generación de soluciones de seguridad cibernética, proporcionando así un impulso al mercado en respuesta a dichos factores.

Conforme lo anterior, la fuente ibidem señala que el mercado de ciberseguridad se segmenta:

Por componentes, el mercado se divide en:

- Solución.
- Servicios.

Las soluciones se dividen en inteligencia de amenazas, antivirus/antimalware, cifrado, mitigación de la denegación de servicio distribuida y filtrado web, gestión unificada de amenazas, cortafuegos, sistemas de detección de intrusiones o sistemas de prevención de intrusiones, prevención de pérdida de datos, recuperación en caso de catástrofe entre otros. A su vez, el segmento de servicios se subdivide en seguridad gestionados y profesionales.

En cuanto al despliegue, la industria se segmenta en:

- Cloud.
- On-Premises.

El modelo de despliegue basado en la nube se utiliza más en el mercado de ciberseguridad en comparación con el segmento local, debido a la expansión de la infraestructura de computación en la nube y a la rápida administración de los servicios de restauración de datos.

En cuanto al despliegue al tipo de seguridad, el mercado de ciberseguridad se divide en:

- Seguridad en la Nube.
- Seguridad de Aplicaciones.
- Seguridad de Endpoints.
- Seguridad de Datos.
- Seguridad de Redes.
- Protección de Infraestructuras.
- Otros.

Basado en tamaño de la organización, el mercado se puede segmentar en:

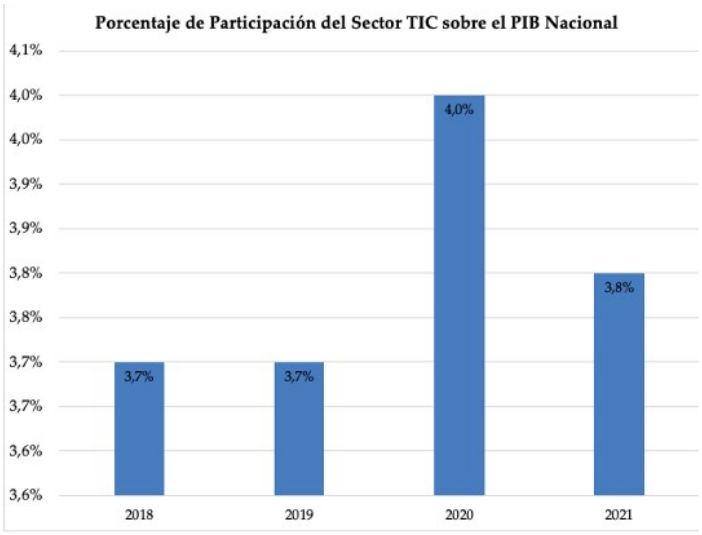
- Grandes Empresas.
- Pequeñas y Medianas Empresas.

Según el uso final, el mercado se segmenta en:

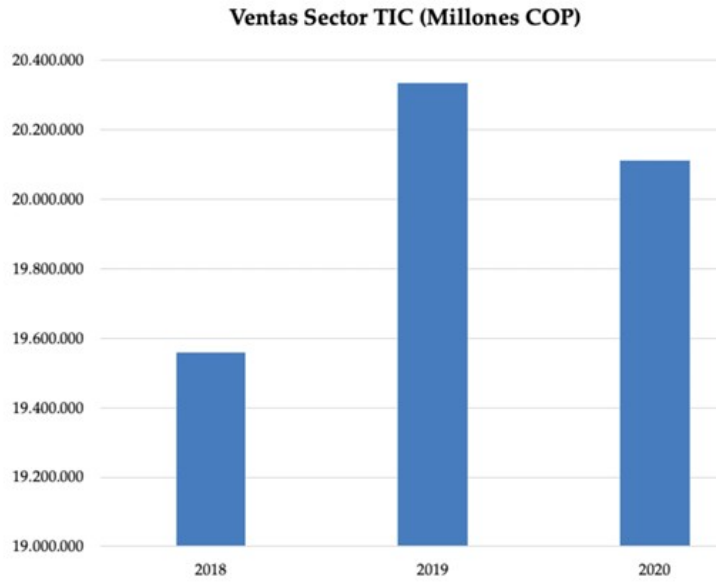
- BFSI.
- Gobierno y Defensa.
- Energía y Servicios Públicos.
- Sanidad.
- TI y Telecomunicaciones.
- Fabricación.
- Comercio minorista.
- Otros.

Siguiendo a Soto y Cifuentes, el sector de las Tecnologías de Información y Comunicaciones presentaba los siguientes datos a 2021:

- ✓ Porcentaje de participación del sector TIC del PIB nacional:



- ✓ Ventas:



Valor agregado de las actividades:



En:https://repository.javeriana.edu.co/bitstream/handle/10554/64394/Propuesta%20comercial%20para%20aumentar%20los%20ingresos%20de%20las%20cuentas%20de%20Trellix%20Colombia%20con%20facturación%20menor%20a%20USD%20%241.000.pdf?sequence=5&isAllowed=y.

2.4. EMPRESAS DE CIBERSEGURIDAD EN COLOMBIA

En armonía con los apartados precedentes, el mercado de la ciberseguridad en Colombia alcanzó un valor de alrededor de USD 279,71 millones para 2023. Se prevé que dicho mercado crezca a una tasa anual compuesta del 14,7% entre 2024 y 2032, para alcanzar un valor de 961,11 millones de USD en 2032, esto como consecuencia de los ataques contra empresas y entidades públicas.

En el mercado interno los principales actores y proveedores de servicios de seguridad son compañías multinacionales que tienen en Colombia un punto de expansión dentro del mercado latinoamericano, donde se destacan Accenture plc, Cisco Systems Inc., CyberArk Software Ltd., Claro Enterprise Solutions, LLC, DigiSOC, Dell Technologies Inc., Sonda S.A., IBM Corporation, Fortinet Inc., entre otras empresas que prestan servicios digitalmente sin domicilio físico en el país.

En Colombia la industria de la ciberseguridad de origen local tiene un bajo nivel de desarrollo. Actualmente la Asociación Colombiana de Ingenieros de Sistemas identifica unas 165 Mipymes en este sector, donde la mayoría se dedica a prestar servicios de consultoría para implementación de productos de grandes empresas internacionales o a ser canal intermediario de las mismas. Es decir, que hay poco o ningún desarrollo de productos y servicios de origen local.

Dichas organizaciones se enfrentan a competidores internacionales muy fuertes, situación que en muchas ocasiones hace que su posición competitiva resulte débil y por tanto sus opciones de crecimiento limitadas. Por ello se hace necesario que las Mipymes nacionales y los emprendimientos que se dedican a prestar servicios de ciberseguridad se fortalezcan, así el ecosistema TIC podrá hacerse fuerte y sostenible. Este proceso de fortalecimiento debe apuntar a que un número significativo de prestadores de servicios del sector de ciberseguridad desarrollen competencias empresariales, habilidades comerciales y capacidad técnica para enfrentar la dinámica de cambio que caracteriza el negocio. Así mismo, dicho proceso debe procurar una conexión real con los sectores y actividades económicas críticas para el funcionamiento digital del país.

Conforme las líneas de acción que precave el Plan Nacional de Desarrollo 2022-2026 *"Colombia, Potencia Mundial de la Vida",* el gobierno busca mejorar las capacidades y fortalecer la cultura de ciberseguridad. Este esfuerzo se plantea como esencial para proteger tanto la información gubernamental como la personal frente a posibles ataques cibernéticos y delitos informáticos. Además, se busca promover un entorno robusto de seguridad digital que asegure la continuidad de los servicios públicos y refuerce la implementación de estándares y buenas prácticas.

En este sentido, el Plan el fijó dentro de los indicadores de segundo nivel, una meta de 20.000 empresas y/o empresarios que adoptan tecnologías para la Transformación Digital, implicando para el cumplimiento de esta, impactar 5.000 beneficiarios por vigencia. Para el año 2024, este proyecto de inversión espera impactar el 10% de la meta establecida para la vigencia, es decir 500 empresas Mipymes beneficiarias.

El proyecto que motiva este análisis está sustentado en la necesidad de promover el desarrollo de la industria nacional de ciberseguridad a través de la generación de las condiciones que permitan en el futuro cercano la creación de un HUB de Ciberseguridad capaz de promover, tanto la oferta como la demanda del negocio como contribución al fortalecimiento de la ciberseguridad en Colombia. En dicho escenario, se espera que resulte posible agrupar empresas grandes, medianas y pequeñas para que a partir de alianzas (técnicas, humanas, comerciales, etc.) se impulse el desarrollo del sector mejorando sus capacidades.

Se anota que la formulación del proyecto que se pretende ejecutar se dio en el marco del Convenio 1257 de 2023 suscrito entre MinTic y el Centro de Bioinformática y Biología Computacional de Colombia - BIOS.

3. GENERALIDADES

Este proyecto se fundamenta en la necesidad de comprender los retos tecnológicos que enfrentan las MIPYMES del país en materia de ciberseguridad y las capacidades del sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo de este modo al fortalecimiento de un ecosistema que aproveche el conocimiento y las tendencias tecnológicas para estimular las dinámicas de oferta y demanda en torno al negocio de la ciberseguridad.

El objetivo general se encuentra enfocado como un proyecto en Ciencia, Tecnológica e Innovación, estando alineado con 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"*, que en su artículo 2, literal h) el cual menciona, lo siguiente: *"Asesorar la negociación, aplicación y adaptación de tecnologías nacionales y extranjeras",* apartado según el cual resulta valida de la celebración de convenios de cooperación entre una entidad gestora (Aliado) y el Ministerio. Este Decreto establece incentivos y estímulos para la inversión en proyectos de ciencia y tecnología en Colombia.

Al promover el desarrollo tecnológico, se incrementa la creación y uso de sistemas informáticos y redes de comunicación, los cuales requieren una sólida infraestructura de ciberseguridad para garantizar su operación segura y eficiente. La ciberseguridad asegura que las innovaciones y los avances tecnológicos no sean vulnerables a ataques cibernéticos, protegiendo tanto la propiedad intelectual como la integridad de los datos y sistemas que son fundamentales para el progreso científico y tecnológico. En este sentido, el proyecto piloto de ciberseguridad aprovecha las tendencias tecnológicas para validar soluciones innovadoras que contribuyen a fortalecer y consolidar el ecosistema de empresas de tecnologías de la información como referente en soluciones de ciberseguridad, en coherencia con el Decreto 391 de 1991.

Adicionalmente, también se hace constar que los objetivos específicos responden a su vez al catálogo de actividades científicas y tecnológicas contenido en el artículo 2 del Decreto 591 de 1991 *"Por el cual se regulan las modalidades específicas de contratos de fomento de actividades científicas y tecnológicas"*, así:

No. 1: Conformación de redes de investigación e información (numeral 1 del artículo ibidem).
No. 2: Transferencia tecnológica que comprende la negociación, apropiación, desagregación, asimilación, adaptación y aplicación de nuevas tecnologías nacionales o extranjeras (numeral 5 del artículo ibidem).
No. 3: Proyectos de innovación que incorporen tecnología, creación, generación, apropiación y adaptación de esta (numeral 4 del artículo ibidem).
No. 4: Cooperación científica y tecnológica nacional (numeral 6 del artículo ibidem).

Este Decreto 591 de 1991 reglamenta el funcionamiento del Sistema Nacional de Ciencia y Tecnología (SNCyT) y establece lineamientos para la coordinación de actividades relacionadas con la investigación y desarrollo tecnológico. La Ciberseguridad se relaciona con este marco al proporcionar las salvaguardas necesarias para proteger la información y los resultados de investigaciones científicas. Además, garantiza la continuidad operativa de las infraestructuras tecnológicas y de información, promoviendo un entorno seguro.

ALCANCE TÉCNICO DEL PROYECTO

Este proyecto se fundamenta en la necesidad de comprender los retos tecnológicos que enfrentan las MIPYMES del país en materia de ciberseguridad y las capacidades del sector de las industrias de tecnologías de la información para atender de manera innovadora estos retos, contribuyendo de este modo al fortalecimiento de un ecosistema que aproveche el conocimiento y las tendencias tecnológicas para estimular las dinámicas de oferta y demanda en torno al negocio de la ciberseguridad.

Por tanto, el proyecto se llevará a cabo para lograr los siguientes objetivos:

4.1 Objetivos del proyecto

El objetivo general del proyecto es implementar una estrategia piloto basada en actividades de transferencia de conocimiento, difusión y adopción tecnológica que permita identificar y plantear soluciones innovadoras a retos tecnológicos en materia de ciberseguridad para ser resueltos por empresas del sector de tecnologías de la información.

Para este fin, se plantean los siguientes objetivos específicos:

1. Identificar, clasificar y definir retos tecnológicos en materia de ciberseguridad, tomando como grupo focal un conjunto de MIPYMES colombianas en las que se identifiquen necesidades de seguridad de la información.

2. Mapear y seleccionar empresas del sector de tecnologías de la información con potencial para desarrollar soluciones en materia de ciberseguridad y fortalecer sus capacidades mediante actividades de transferencia de conocimiento para atender los retos tecnológicos identificados.

3. Plantear e implementar soluciones innovadoras a los retos identificados, mediante procesos de transferencia tecnológica entre las MIPYMES y las empresas del sector de tecnologías de la información.

4. Generar espacios de difusión tecnológica para fortalecer las capacidades del país en materia aplicación y adaptación de tecnologías de ciberseguridad.

4.2 Fases del proyecto

Para el desarrollo del proyecto se plantean las siguientes fases con sus actividades, resultados esperados y entregables. Los plazos de presentación de los entregables, para aprobación del supervisor designado por parte del Ministerio, corresponden a los plazos límite contados a partir de la fecha de suscripción del contrato.

Fase 1. Planeación y alistamiento

En esta fase se definirá el plan detallado de trabajo, las herramientas y plataformas que se utilizarán para soportar la ejecución y seguimiento de las actividades del proyecto. Así mismo, se conformará el equipo de trabajo que ejecutará el proyecto.

	Actividades	Resultados	Entregables
Fase 1. Planeación y alistamiento	**Actividad 1.1** Elaborar el plan de trabajo de detallado para ejecutar las actividades del proyecto en un plazo de hasta cuatro meses, en todo caso sin sobrepasar el 31 de diciembre del 2024.	**Resultado 1.1** El plan de trabajo detallado para la ejecución técnica y financiera del proyecto.	**Entregable 1.1** Plan de trabajo detallado que incluya todas las fases del proyecto y con un cronograma que considere los momentos de los entregables, los hitos, entregas de informes, desembolsos y demás aspectos del proyecto.
	Actividad 1.2 Definir el equipo de trabajo mediante la selección de las personas que lo integrarán y presentar sus perfiles al Ministerio de Tecnologías de la Información y las Comunicaciones para validación.	**Resultado 1.2** Equipo de trabajo del proyecto definido.	**Entregable 1.2** Matriz que recopile cada uno de los perfiles seleccionados junto con las hojas de vida de cada perfil.

Fase 2. Definición de retos tecnológicos

En esta fase se identificarán, clasificarán y definirán los retos tecnológicos en materia de ciberseguridad de un grupo de 100 MIPYMES colombianas en las que se identifiquen necesidades de seguridad de la información, seleccionadas mediante una convocatoria.

<table>
<tr><td colspan="4">Objetivo Específico 1: Identificar, clasificar y definir retos tecnológicos en materia de ciberseguridad, tomando como grupo focal un conjunto de MIPYMES colombianas en las que se identifiquen necesidades de seguridad de la información.</td></tr>
<tr><th>Fase 2.
Definición de retos tecnológicos</th><th>Actividades</th><th>Resultados</th><th>Entregables</th></tr>
<tr><td rowspan="5"></td><td rowspan="3">Actividad 2.1 Realizar una convocatoria dirigida a MIPYMES constituidas en Colombia, de cualquier sector económico, que requieran soluciones de ciberseguridad.</td><td rowspan="3">Resultado 2.1 Una (1) convocatoria realizada a nivel nacional que vincule al menos cien (100) empresas que tengan una necesidad tecnológica en ciberseguridad.</td><td>Entregable 2.1 Plan operativo de la convocatoria que incluya, entre otros elementos, la estrategia de comunicación y divulgación, los mecanismos para la identificación y vinculación de empresas, la metodología e instrumentos para la inscripción y validación de empresas y el cronograma del proceso.</td></tr>
<tr><td>Entregable 2.2 Términos de referencia de la convocatoria dirigida a las MYPES que desean participar en el proyecto.</td></tr>
<tr><td>Entregable 2.3 Informe de implementación de la convocatoria en las que se incluya tanto las empresas inscritas, como las que participan en el proceso de las 100 empresas vinculadas. (empresas seleccionadas).</td></tr>
<tr><td>Actividad 2.2 Identificar y clasificar los retos tecnológicos de ciberseguridad de cada MIPYME, realizando la clasificación según las categorías de ciberseguridad y tipo de innovación</td><td rowspan="2">Resultado 2.2 Al menos cien (100) retos con sus respectivas fichas de caracterización estructuradas, una para cada empresa vinculado en la convocatoria.</td><td rowspan="2">Entregable 2.4 Un banco de al menos cien (100) retos con sus respectivas fichas de caracterización estructuradas, una para cada empresa, que incluya un planteamiento de las temáticas necesarias a desarrollar en los procesos de transferencia de conocimiento de la Fase 3</td></tr>
<tr><td>Actividad 2.3 Conformar un banco de retos a solucionar con la caracterización detallada de cada reto que incluya, entre otros, el alcance, el problema, los recursos científicos, técnicos y tecnológicos mínimos</td></tr>
</table>

	necesarios para resolver el problema y los resultados esperados.		

Fase 3. Fortalecimiento de solucionadores tecnológicos

En esta fase se seleccionarán hasta 45 empresas del sector de tecnologías de la información que tengan potencial para desarrollar soluciones en materia de ciberseguridad, con el fin de fortalecer sus capacidades mediante actividades de transferencia de conocimiento para atender los retos tecnológicos identificados en la Fase 2.

Objetivo Específico 2: Mapear y seleccionar empresas del sector de tecnologías de la información con potencial para desarrollar soluciones en materia de ciberseguridad y fortalecer sus capacidades mediante actividades de transferencia de conocimiento para atender los retos tecnológicos identificados.			
Fase 3. Fortalecimiento de solucionadores tecnológicos	**Actividades**	**Resultados**	**Entregables**
	Actividad 3.1 Realizar una convocatoria dirigida a empresas del sector de tecnologías de la información en ciberseguridad en Colombia para fortalecerlas en tendencias de ciberseguridad, y seleccionar hasta cuarenta y cinco (45) empresas con potencial para desarrollar soluciones en ciberseguridad mediante un análisis de su portafolio, capacidades y experiencia.	**Resultado 3.1** Una (1) convocatoria realizada a nivel nacional que vincule hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad.	**Entregable 3.1** Plan operativo de la convocatoria que incluya, entre otros elementos, la estrategia de comunicación y divulgación, los mecanismos para la identificación y vinculación de empresas, la metodología e instrumentos para la inscripción y validación de empresas y el cronograma del proceso.
			Entregable 3.2 Términos de referencia de la convocatoria con los criterios de selección de las empresas de tecnologías de la información.
			Entregable 3.3 Informe de implementación de la convocatoria que dé cuenta del proceso de selección y vinculación de las 45 empresas de tecnologías de la información vinculadas.
	Actividad 3.2 Realizar un mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica), que permita identificar herramientas, prácticas, modelos de negocio innovadores y tendencias para facilitar los procesos de transferencia de conocimiento en las soluciones de los retos.	**Resultado 3.2** Un (1) mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica).	**Entregable 3.4** Documento con el resultado del mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica), que incluya la identificación de herramientas, prácticas, modelos de negocio innovadores y tendencias para tener en cuenta en los procesos de transferencia de conocimiento.
	Actividad 3.3 Diseñar e implementar un plan de transferencia de	**Resultado 3.3** Cinco (5) micro cursos (micro acreditaciones)	**Entregable 3.5** Plan de transferencia de conocimiento para las 45 empresas de tecnologías de la información vinculadas,

		de ciberseguridad desarrollados, de diez (10) horas cada uno, dirigidos a las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información seleccionadas, con la participación de una persona por empresa, en temáticas basadas en el estudio de vigilancia tecnológica sobre tendencias actuales en ciberseguridad.	sobre los micro cursos, el bootcamp y las mentorías especializadas, que incluya, entre otros elementos, los contenidos a desarrollar, las metodologías a implementar, las herramientas tecnológicas a utilizar, el cronograma y la intensidad horaria de las actividades, los mecanismos de control, evaluación y validación de la efectividad de la transferencia.
	conocimiento para el fortalecimiento de las empresas de tecnologías de la información, que incluya cursos cortos (micro acreditaciones), la realización de un *bootcamp* y sesiones de mentoría especializada dirigidas a las empresas solucionadoras seleccionadas.	**Resultado 3.4** Un (1) *bootcamp* de 20 horas sobre seguridad digital desarrollado para las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información seleccionadas, con la participación de una persona por empresa.	**Entregable 3.6** Informe de implementación del plan de transferencia de conocimiento para las 45 empresas de tecnologías de la información vinculadas, que incluya, entre otros elementos, las listas de asistencia, las memorias de los cursos, el bootcamp y las mentorías especializadas (* un apartado por cada actividad), grabaciones, las certificaciones o reconocimientos otorgados a las empresas participantes, encuestas de satisfacción y evaluación realizadas por las empresas beneficiarias, y lecciones aprendidas u oportunidades de mejora para un eventual escalamiento del proyecto.
		Resultado 3.5 Cuatro (4) horas de mentoría especializada e individualizada para cada una de las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad seleccionadas, enfocadas en metodologías de innovación para la solución de los retos tecnológicos planteados.	

Fase 4. Implementación de retos tecnológicos

En esta fase se implementarán soluciones innovadoras a los retos de ciberseguridad de al menos diez (10)

MIPYMES seleccionadas del banco conformado en la Fase 1 del proyecto, mediante procesos de transferencia tecnológica desarrollados por las empresas del sector de tecnologías de la información fortalecidas en la Fase 2.

<table>
<tr><td colspan="4">Objetivo Específico 3: Plantear e implementar soluciones innovadoras a los retos identificados, mediante procesos de transferencia tecnológica entre las MIPYMES y las empresas del sector de tecnologías de la información.</td></tr>
<tr><td rowspan="5">Fase 4.
Implementación de retos tecnológicos</td><td>Actividades</td><td>Resultados</td><td>Entregables</td></tr>
<tr><td rowspan="2">Actividad 4.1
Diseñar soluciones para los retos tecnológicos, con al menos una solución propuesta por cada empresa del sector de tecnologías de la información fortalecida en la Fase 2.</td><td rowspan="2">Resultado 4.1 Al menos cuarenta y cinco (45) propuestas de soluciones para retos tecnológicos de MIPYMES del banco conformado en la Fase 2, planteadas por las empresas del sector de tecnologías de la información fortalecidas en la Fase 3.</td><td>Entregable 4.1 Modelo o formato de ficha para la presentación de propuesta de solución de retos.</td></tr>
<tr><td>Entregable 4.2 Un banco de al menos cuarenta y cinco (45) propuestas de soluciones, conformado con las soluciones propuestas por las empresas del sector de tecnologías de la información fortalecidas, con las respectivas fichas de solución que incluya, entre otros aspectos, la metodología de solución, recursos científicos, técnicos y tecnológicos a utilizar y el componente innovador de la solución diseñadas por las empresas.</td></tr>
<tr><td rowspan="3">Actividad 4.2
Implementar las soluciones para los retos de al menos diez (10) MIPYMES seleccionadas (retadoras) del banco conformado en la Fase 2.</td><td rowspan="3">Resultado 4.2 Al menos diez (10) retos de ciberseguridad solucionados para las MIPYMES seleccionadas (retadoras), por parte de empresas del sector de tecnologías de la información.</td><td>Entregable 4.3 Documento de lineamientos operativos para la selección de las diez (10) MIPYMES y sus retos, los criterios para los emparejamientos de solucionador-retador, las condiciones contractuales, técnicas y jurídicas para estos emparejamientos, el mecanismo de operación del desarrollo de las soluciones, entre otros.</td></tr>
<tr><td>Entregable 4.4 Diez (10) fichas de ejecución de las soluciones tecnológicas implementadas, que describan las metodologías utilizadas, los servicios tecnológicos y las capacidades transferidas a las empresas, los resultados e impactos de la solución, oportunidades, etc.</td></tr>
<tr><td>Entregable 4.5 Informe general de todo el proceso desarrollado en la Fase 4, que incluya como mínimo los resultados generales, las lecciones aprendidas y las oportunidades de mejora para una eventual replicación o escalamiento del proyecto.</td></tr>
</table>

Fase 5. Difusión y cierre

En esta fase se llevará a cabo un evento de divulgación tecnológica para el ecosistema de ciberseguridad, con el fin de fortalecer las capacidades del país en materia de aplicación y adaptación de tecnologías de ciberseguridad.

Objetivo Específico 4: Generar espacios de difusión tecnológica para fortalecer las capacidades del país en materia aplicación y adaptación de tecnologías de ciberseguridad.			
Fase 5. Difusión y cierre	**Actividades**	**Resultados**	**Entregables**
	Actividad 5.1 Organizar y desarrollar un evento académico y colaborativo en temas de ciberseguridad para un aforo de 80 personas, con una duración de hasta tres días y participación de expertos nacionales e internacionales para abordar las últimas tendencias tecnológicas, desafíos y estrategias en ciberseguridad. Con una agenda compuesta de conferencias, conversatorios y sesiones de networking que apunte a fortalecer las capacidades en ciberseguridad de profesionales, académicos y estudiantes, fomente la cooperación y el intercambio de conocimientos. Además, con stands empresariales y académicos, promoviendo la innovación y el desarrollo en el campo de la seguridad informática.	**Resultado 5.1** Un evento académico y colaborativo en temas de ciberseguridad para un aforo de 80 personas, con una duración de tres días y participación de expertos nacionales e internacionales para abordar las últimas tendencias tecnológicas, desafíos y estrategias en ciberseguridad.	**Entregable 5.1** Plan de organización y desarrollo del evento que incluya, entre otros aspectos, la planeación logística, cotizaciones y proveedores, las listas de invitados y conferencistas, los temas y actividades a desarrollar y la agenda académica. **Entregable 5.2** Informe de realización del evento que incluya las memorias, listas de asistencia y registros audiovisuales.
	Actividad 5.2. Desarrollar una herramienta tecnológica para hacer seguimiento y control del proyecto	**Resultado 5.2.** Herramienta virtual en la nube desarrollada para seguimiento y gestión del proyecto y visibilización de las innovaciones en ciberseguridad, que incluya los siguientes módulos: Módulos Backend (5) 1. Gestión de Usuarios y Autenticación: 2. Gestión de Proyectos 3. Base de Datos de Empresas y MIPYMES 4. Gestión de Retos Tecnológicos. Transferencia de	**Entregable 5.3.** Herramienta virtual en la nube desarrollada para seguimiento y gestión del proyecto y visibilización de las innovaciones en ciberseguridad.

		Conocimiento 5. Gestión de propuestas de soluciones innovadoras. Módulos Frontend (6) 1. Dashboard Principal 2. Gestión de Usuarios 3. Visualización de Proyectos 4. Empresas y MIPYMES 5. Retos Tecnológicos 6. Eventos y Difusión	

4. TRAYECTORIA DE BIOS

La siguiente tabla resume la experiencia de BIOS como ejecutor de proyectos para MinTIC.

#	PROYECTO	OBJETO	ENTIDAD	FECHA INICIO	DURACIÓN	VALOR
1	Centro de inteligencia artificial aplicada	Aunar esfuerzos técnicos administrativos y financieros para el desarrollo de proyectos de ciencia tecnología e innovación con énfasis en los sectores estratégicos de las Direcciones del gobierno en línea, políticas y Desarrollo de TI, I+D+I, que permitan el desarrollo de los objetivos planteados en el plan estratégico del Min TIC	MinTIC	23/08/2017	12 meses	$ 7.944.877.927
2	Diseñar el Centro de Servidos Compartidos de Transformación Digital (CSCTD) para la atención de retos institucionales o empresariales a partir del uso de nuevas tecnologías tales como Inteligencia Artificial, el rediseño de los centros de excelencia y apropiación en BigData, IoT de conformidad a las Hojas de Ruta Regionales de Transformación Digital	"Diseñar el Centro de Servidos Compartidos de Transformación Digital (CSCTD) para la atención de retos institucionales o empresariales a partir del uso de nuevas tecnologías tales como Inteligencia Artificial, el rediseño de los centros de excelencia y apropiación en BigData, IoT de conformidad a las Hojas de Ruta Regionales de Transformación Digital, garantizando la formulación y ejecución de proyectos que brinden soluciones a los sectores de la economía que coadyuven al desarrollo de las empresas en sus diferentes iniciativas regionales y nacionales. Toda la información resultante usará las capacidades e infraestructura computacional de alto desempeño con la que actualmente cuenta BIOS"	FONTIC	19/12/2019	12 meses	$ 1.970.966.877
3	Implementación de la Red Nacional de Supercomputación	El objetivo principal del convenio especial de cooperación es aunar esfuerzos técnicos, administrativos y financieros, para realizar las acciones y estrategias correspondientes para la creación y articulación de la Red Nacional de Servicios de	MinTIC	18/02/2021	10 meses	$ 1.231.948.648

		Computación de Alto Rendimiento				
4	Resolución 00528: Por la cual se ordena un gasto como aporte	Por la cual se ordena un gasto como aporte al Centro de Bioinformática y Biología Computacional de Colombia o BIOS o CBBC con NIT 900.404.482-6	MINTIC	24/07/2023	5 meses	$ 1.500.000.000
5	Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.	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.	MINTIC	17/11/2023	1 mes y medio	$ 5.100.000.000

5. EQUIPO DE TRABAJO

Se contratará un equipo de trabajo base multidisciplinario con dedicación exclusiva, para garantizar la implementación y el cumplimiento del proyecto. A continuación se enuncian roles y su función principales en el desarrollo del proyecto:

Rol	Función
Gerente del proyecto (1)	_Construir el Plan operativo y contrataciones _Seguimiento actividades _Generación de informes
Líder Administrativo y Financiero (1)	_ Ejecución financiero del proyecto _ Informes de ejecución
Asesor Legal (1)	_Liderar estrategia legal de todo el proyecto _Consolidar TR, carta de compromiso y tratamiento de datos que se aplicarán en las convocatorias
Líder de Tecnología (1)	_ Liderar la generación de las propuestas de soluciones innovadoras en colaboración con las empresas seleccionadas
Profesionales Expertos en ciberseguridadn (5)	_Creación del isntrumento de clasificación de retos y capacidades proveedores _Creación del informe de resultados Retos _Consolidación del banco de reto _Creación del informe del portencial de las empresas _ Implementar diez (10) pilotos de las soluciones propuestas en un grupo de MIPYMES _ Obtener retroalimentación de la solución implementada y realizar ajustes necesarios
Líder Comunicaciones Divulgación Tecnológica (1)	_Diseñar y liderar la estrategia de divulgación _ Diseñar el plan de transferencia de conocimiento que incluya micro-

	acreditaciones, bootcamps y horas de mentoría dirigidas a las empresas solucionadoras _ Organizar y desarrollar un evento académico y colaborativo en temas de ciberseguridad con el líder de formación
Profesional Líder transferencia de conocimiento (1)	_Creación de los TR, Tratamiento de datos (con apoyo del asesor legal) y sociodemografico _Convocatoria oferta y demanda _Convocatoria evento de formación _Creación plan de transferencia de conocimiento que incluya micro-acreditaciones, bootcamps y horas de mentoría dirigidas a las empresas solucionadoras _ Organizar y desarrollar un evento académico y colaborativo en temas de ciberseguridad.

6. PRESUPUESTO ESTIMADO

El presupuesto global asciende a la suma de $2.085.082.969 (dos mil ochenta y cinco millones ochenta y dos mil novecientos sesenta y nueve pesos), de los cuales $198.130.056 (ciento noventa y ocho millones ciento treinta mil cincuenta y seis pesos) corresponden a aportes en contrapartida en especie por parte de BIOS, representados en recurso humano para el desarrollo de actividades técnicas y de administración del proyecto, y $1.886.952.913 (Mil ochocientos ochenta y seis millones novecientos cincuenta y tres mil novecientos trece pesos) corresponden a aportes de MinTIC, desglosados según los entregables, como se presenta en la siguiente tabla.

COMPONENTE	ACTIVIDAD	RESULTADO ESPERADO	UNIDAD	CANTIDAD	VALOR (CON IVA)	VALOR TOTAL
Fase 1. Planeación y alistamiento	Actividad 1.1 Elaborar el plan de trabajo de detallado para ejecutar las actividades del proyecto en un plazo de hasta cuatro meses, en todo caso sin sobrepasar el 31 de diciembre del 2024.	Resultado 1.1 El plan de trabajo detallado para la ejecución técnica y financiera del proyecto.	Plan de trabajo	1	-	-
	Actividad 1.2 Definir el equipo de trabajo mediante la selección de las personas que lo integrarán y presentar sus perfiles al Ministerio de Tecnologías de la Información y las Comunicaciones para validación.	Resultado 1.2 Equipo de trabajo del proyecto definido.	Equipo base	1	-	-
Fase 2. Identificación, clasificación y conformación de retos tecnológicos.	Actividad 2.1. Realizar una convocatoria dirigida a MIPYMES	Una convocatoria realizada a nivel nacional que vincule al menos cien (100) empresas que tengan una necesidad	Convocatoria	1	$ 131.562.651	$ 131.562.651

	constituidas en Colombia, de cualquier sector económico, que busquen fortalecer sus capacidades en ciberseguridad.	tecnológica en ciberseguridad.				
	Actividad 2.2. Identificar y clasificar los retos tecnológicos de ciberseguridad de cada MIPYME	Un banco de al menos cien (100) retos con sus respectivas fichas de caracterización estructuradas, una para cada empresa, que incluya un análisis de temáticas para desarrollar en el proceso de transferencia de conocimiento.	Empresas	100	$ 658.664	$ 65.866.400
	Actividad 2.3. Conformar un banco retos a solucionar con la caracterización detallada de cada reto que incluya, entre otros, el alcance, el problema, los recursos científicos, técnicos y tecnológicos mínimos necesarios para resolver el problema y los resultados esperados.			100	$ 450.972	$ 45.097.200
Fase 3. Mapeo, selección y fortalecimiento de solucionadores tecnológicos.	Actividad 3.1. Realizar una convocatoria dirigida a empresas del sector de tecnologías de la información en ciberseguridad en Colombia para fortalecerlas en tendencias de ciberseguridad, y seleccionar hasta cuarenta y cinco (45) empresas con potencial para desarrollar soluciones en ciberseguridad mediante análisis de su portafolio, capacidades y experiencia.	Una convocatoria realizada a nivel nacional que vincule hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad.	Convocatoria	1	$ 167.046.179	$ 167.046.179
	Actividad 3.2. Realizar un mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia	Un mapeo sobre las tecnologías e innovaciones de punta en ciberseguridad (vigilancia tecnológica) que permita identificar herramientas, prácticas, modelos de negocio innovadores y	Documento	1	$ 121.155.007	$ 121.155.007

	tecnológica), que permita identificar herramientas, prácticas, modelos de negocio innovadores y tendencias para facilitar los procesos de transferencia de conocimiento en las soluciones de los retos.	tendencias para facilitar la posterior transferencia de conocimiento.				
	Actividad 3.3. Diseñar e implementar un plan de transferencia de conocimiento que incluya cursos cortos (microacreditaciones), la realización de un bootcamp y sesiones de mentoría especializada dirigidas a las empresas solucionadoras seleccionadas.	Cinco (5) microcursos (microacreditaciones) de diez (10) horas cada uno diseñados e implementados, dirigidos a las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad seleccionadas, una persona por empresa en temáticas basadas en el estudio de vigilancia tecnológica sobre tendencias actuales en ciberseguridad.	Microacreditaciones (5 por empresa)	225	$ 597.000	$ 134.325.000
		Un bootcamp desarrollado de 20 horas para las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad seleccionadas, una persona por empresa, en seguridad digital.	Bootcamp	1	$ 55.750.000	$ 55.750.000
		Cuatro (4) horas de mentoría especializada e individualizada para cada una de las hasta cuarenta y cinco (45) empresas del sector de tecnologías de la información en ciberseguridad seleccionadas, enfocadas en metodologías de innovación para la solución de los retos tecnológicos planteados.	Empresas	45	$ 2.088.000	$ 93.960.000
Fase 4. Diseño e implementación de soluciones innovadoras.	Actividad 4.1. Diseñar soluciones para los retos tecnológicos, con al menos una solución propuesta por cada empresa del sector de tecnologías de la información	Un banco de al menos cuarenta y cinco (45) propuestas de soluciones, conformado con las soluciones propuestas por las empresas del sector de tecnologías de la información fortalecidas, con las respectivas fichas de solución que incluya, entre otros aspectos, la metodología de solución,	Proyectos (Fichas de soluciones)	45	$ 2.386.774	$ 107.404.830

	fortalecida en el Componente 2.	recursos científicos, técnicos y tecnológicos a utilizar y el componente innovador de la solución diseñadas por las empresas.				
	Actividad 4.2. Implementar las soluciones para los retos de al menos diez (10) MIPYMES seleccionadas del banco conformado en el Componente 1.	Diez (10) retos de ciberseguridad solucionados para las MIPYMES seleccionadas del banco de propuestas de soluciones, por parte de empresas del sector de tecnologías de la información.	Proyectos Implementados	10	$ 65.000.000	$ 650.000.000
Fase 5. Difusión tecnológica para el ecosistema de ciberseguridad.	5.1 Organizar y desarrollar un evento académico y colaborativo en temas de ciberseguridad para un aforo de 80 personas, con una duración de tres días y participación de expertos nacionales e internacionales para abordar las últimas tendencias tecnológicas, desafíos y estrategias en ciberseguridad. Con una agenda compuesta de conferencias, conversatorios y sesiones de networking que apunte a fortalecer las capacidades en ciberseguridad de profesionales, académicos y estudiantes, fomente la cooperación y el intercambio de conocimientos. Además, con stands empresariales y académicos, promoviendo la innovación y el desarrollo en el campo de la seguridad informática.	Un evento académico y colaborativo en temas de ciberseguridad para un aforo de 80 personas, con una duración de tres días y participación de expertos nacionales e internacionales para abordar las últimas tendencias tecnológicas, desafíos y estrategias en ciberseguridad.	Evento	1	$ 253.716.005	$ 253.716.005

	5.2 Desarrollo de una herramienta tecnologica para hacer seguimiento y control del proyecto.	Herramienta virtual en la nube desarrollada para seguimiento y gestión del proyecto y visibilización de las innovaciones en ciberseguridad	Herramienta virtual	1	$ 61.069.641	$ 61.069.641
TOTAL GENERAL						**$ 1.886.952.913**

Contrapartida

A continuación se detallan los rubros de contrapartida, correspondientes al personal de BIOS que se vinculará al proyecto.

CONCEPTO	JUSTIFICACION	VALOR
TALENTO HUMANO	Dos (2) profesionales con maestría y amplia experiencia en desarrollo de metodologías ágiles para la ejecución de las actividades del proyecto	$ 142.243.225
	Un (1) profesional para el apoyo y seguimiento a los retos de ciberseguridad	$ 22.862.794
	Un (1) profesional con maestría para la elaboración del plan operativo del proyecto	$ 33.024.037
TOTAL CONTRAPARTIDA		**$ 198.130.056**

7. SEGURIDAD DE LA INFORMACIÓN.

El Aliado (ejecutor) deberá tener implementado un modelo de seguridad de la información y alienar sus procesos y procedimientos internos relacionados con la ejecución del presente proyecto, alineado con lo definido en lo referente a Seguridad y Privacidad de la Información por parte del MinTic, teniendo en cuenta lo definido en los apartados que integran el presente capítulo.

Se debe mantener la confidencialidad de la información propiedad de la entidad a que tenga acceso en el marco de ejecución del contrato, así mismo cuando termine el contrato deberá entregar a la entidad toda la información que este solicite garantizando que la misma es propiedad de la entidad. El Aliado (ejecutor) se compromete a no divulgar la información obtenida durante la ejecución del contrato a terceras personas.

El personal asociados al Aliado (ejecutor) a cargo del proyecto, deberá firmar un acuerdo de confidencialidad, para garantizar la reserva de la información a la cual tengan acceso.

Cumplimiento de la Política de Seguridad MinTIC

El Aliado (ejecutor) se debe alinear y cumplir lo establecido en el Sistema de Gestión de la Seguridad de la información que viene implementando el Ministerio TIC, y dar cumplimiento a la Resolución 0448 de 2022, la cual actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad y Continuidad de la Operación de los servicios del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, la cual establece en el su Artículo 2 Ámbito de aplicación:

Política General de Seguridad y Privacidad de la Información, Seguridad y Continuidad de la Operación de los servicios del Ministerio/Fondo único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de las Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen intercambien o consulten su información, al igual que a las entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información independiente de su ubicación. De igual manera, esta política aplica a toda información creada, procesada o utilizada por el Ministerio/Fondo único de TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

De igual manera, a los parámetros establecidos por la Subdirección Administrativa en la Política de Gestión de Activos (Inventario de activos, Protección, Archivos de Gestión, Clasificación de la Información, y firma de documentos) descritos en el Artículo 6 de la resolución señalada.

Políticas de Borrado Seguro

El Aliado (ejecutor) deberá realizar el borrado seguro de cada uno de los dispositivos que sean utilizados en cualquiera de los servicios a desplegarse en las entidades, como parte de la ejecución del contrato.

Al finalizar la ejecución el Aliado (ejecutor) deberá allegar con firma del representante legal, una certificación en la cual se evidencie que en todos los casos en donde se tuvo registro de información y datos de las entidades, fueron objeto de las políticas de borrado seguro, de tal forma que garantice que la información gestionada, almacenada fue eliminada en su totalidad y que no queda ninguna copia o elemento que permita realizar un proceso de recuperación.

Formatos y documentos

El Aliado (ejecutor) deberá diligenciar todos los formatos y documentos fijados por MinTIC conforme lo disponga el modelo integrado de gestión (MIG), entre ellos, acuerdos de confidencialidad firmados por el representante legal, como todo equipo destinado a la ejecución del convenio.

8. CUMPLIMIENTO LEY 1581 DEL 2012

En línea con la disposición de la política de protección de datos personales de MinTic actualizada mediante Resolución 0448 de 2022, el Aliado (ejecutor) debe garantizar el cumplimiento de los dispuesto en dicho acto de conformidad con lo señalado en el parágrafo del Artículo 6: Identificación del responsable y/o

encargado del tratamiento.

MinTic dispone que los titulares de los datos personales cuyo tratamiento realiza el Ministerio, tienen los siguientes derechos:

- Acceder los datos personales que hayan sido objeto de Tratamiento conforme a lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.

- Conocer, actualizar y rectificar los datos personales frente al responsable del Tratamiento y al Encargado del Tratamiento. El derecho de actualizar y rectificar los datos se podrá ejercer, entre otros datos, en relación con datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos datos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

- Solicitar prueba de la autorización otorgada al responsable del Tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.

- Ser informado por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, con respecto del uso que les ha dado a los datos personales. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 en el Decreto 1377 de 2013 y en las demás normas que los modifiquen, adicionen o complementen.

- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la Constitución, a la Ley 1581 de 2012 y a las demás normas que la reglamenten modifiquen o subroguen.



Paula Marcela Arias Pulgarín
Directora Ejecutiva