Requerimiento Técnico

FORTALECIMIENTO DE CAPACIDADES EN SEGURIDAD DIGITAL

1.- Descripción de la necesidad que la entidad pretende satisfacer

La creciente participación de ciudadanos en el entorno digital, la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC), traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital, lo cual exige que el país cuente con suficientes capacidades para su adecuada y oportuna gestión. Las amenazas, los ataques e incidentes de seguridad digital cada día son más sofisticados y complejos e implican graves consecuencias de tipo económico o social.

Se identificó la necesidad de fortalecer y consolidar un entorno digital abierto basado en la confianza y la seguridad para el desarrollo de una sociedad interconectada, teniendo en cuenta las recomendaciones que sobre la materia brinda la OCDE, con el fin de mantener la creación de riqueza, la innovación, el crecimiento, la competitividad y el empleo en todos los sectores de la economía (OECD, 2015).

Como consecuencia de lo mencionado, se expidió en el año 2016, el Documento CONPES 3854 Política Nacional de Seguridad Digital, cuyo objetivo consistió en fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

Adicionalmente, se generaron mecanismos estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional y se crea la figura de Coordinador Nacional de Seguridad Digital.

A pesar de lo anterior, estas políticas se dirigieron principalmente al Gobierno Nacional, siendo baja la gestión frente a convenios y acuerdos de cooperación e intercambio de información con las múltiples partes interesadas y, poco avance respecto a los estudios de viabilidad para la creación de nuevas instancias, en temas relacionados con la defensa y seguridad nacional en el entorno digital.

El Informe Global de Riesgos 2019, presenta que el fraude de datos, los ciberataques y las vulnerabilidades tecnológicas, aparecen como grandes preocupaciones junto a eventos climáticos o desastres naturales, ubicándose dentro de los diez principales riesgos

globales con mayor grado de probabilidad de ocurrencia (Foro Económico Mundial - FEM, 2019).

Por otro lado, según previsiones del Centro para la Ciberseguridad (C4C, por sus siglas en inglés) del FEM, la pérdida económica debida al delito cibernético puede alcanzar los 3 billones de dólares para el año 2020, y el 74 % de las empresas del mundo podrían ser hackeadas el próximo año, mientras que para 2021 se estima que los daños ocasionados por los ciberdelitos alcancen los 6 trillones de dólares (Foro Económico Mundial [FEM], 2020).

Según el reporte Estado de Internet 2019 (Akamai, 2019), entre noviembre de 2017 y septiembre de 2019, en Colombia se originaron alrededor de 536 millones de ataques (contados entre inicio de sesión malicioso y ataques a aplicaciones web).

Respecto a la generación de capacidades a través de la educación formal en materia de seguridad digital, el Índice de Ciberseguridad Nacional en inglés, National Cyber Security Index (NCSI), Colombia en este pilar obtiene un avance del 44 %, lo que muestra un bajo avance al respecto. A través del Sistema Nacional de Información de la Educación Superior (SNIES) del Ministerio de Educación Nacional, se evidencia que existen 41 programas activos relacionados con seguridad digital, de los cuales, 36 son de nivel académico posgrado con sólo 3 maestrías. También se cuentan 5 programas que corresponden a nivel académico pregrado con 4 de formación tecnológica o técnica y 1 programa universitario.

Con base en lo anteriormente expuesto es se considera necesario incrementar la oferta académica en materia de seguridad digital sin descuidar que el acceso a las Tecnologías de la Información y las Comunicaciones (TIC) sea equitativo para todos. Según datos disponibles en 2015 del Observatorio de Tecnologías de la Información (TI)21, la participación de mujeres en empresas de Teleinformática, Software y TI fue del apenas del 39 %, mientras que los hombres representaron un 61 %. En el campo de seguridad digital, el estudio Genero y TIC en América Latina (5G Américas, 2019), resalta cómo las TIC se presentan como una herramienta para mejorar las condiciones de vida de mujeres y niñas y llama la atención sobre la importancia de que se realicen esfuerzos conjuntos entre los sectores públicos y privado para generar diferentes estrategias que busquen potenciar el acceso de las mujeres a las TIC.

En relación con iniciativas de generación de capacidades en materia de seguridad digital, el Ministerio de Tecnologías de la Información y las Comunicaciones adelantó las iniciativas Hacker Girls con apoyo de la OEA y Por TIC Mujer la cual tiene como objetivo empoderar a las mujeres en el uso y apropiación de las TIC.

Por otro lado, algunas específicas de formación en seguridad digital a jóvenes también con apoyo de la OEA, como el programa internacional Creación de una Trayectoria Profesional en Seguridad Digital, dirigido a jóvenes de escasos recursos económicos y estudiantes universitarios de ingeniería. A pesar del desarrollo de estas iniciativas, no se han realizado evaluaciones ni establecido condiciones para gestionar riesgos de seguridad digital de comunidades en condiciones especiales de vulnerabilidad, teniendo en cuenta lo anterior se han considerado necesidades particulares de grupos poblacionales específicos en el marco de un enfoque diferencial, específicamente de jóvenes.

Así las cosas, el comportamiento evidenciado para Colombia deja en claro que las capacidades en seguridad digital no son suficientes para generar cambios notorios en el entorno digital del país, reflejando la necesidad de aumentar dichas capacidades.

Dicho lo anterior, se considera que uno de los principales retos que tiene Colombia en materia de ciberseguridad, es mejorar la confianza y seguridad en los ecosistemas digitales y para ello, es necesario realizar acciones de política para que las múltiples partes interesadas (El Gobierno Nacional y los territorios, las organizaciones públicas y privadas, la fuerza Pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades) en Colombia puedan adelantar sus actividades socioeconómicas en dicho entorno de manera segura y confiable.

Así las cosas, el nuevo CONPES 3995 de Confianza y Seguridad Digital con fecha Julio del 2020 formula una política nacional que tiene como objetivo: 5.1. Objetivo general: "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías. 5.2. Objetivos específicos OE 1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país. OE 2. Actualizar el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y mejorar el avance en seguridad digital del país. OE 3. Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país a los desafíos de la 4R" Según documento CONPES 3995.

Con base en lo establecido en dicho CONPES se han venido realizando una serie de actividades tendientes al fortalecimiento de las capacidades en seguridad digital en el Estado, dirigidas principalmente a los encargados de la seguridad y TI de las entidades públicas, sin embargo con el propósito del documento de política CONPES 3995 de 2020,

se encarga al Ministerio TIC de desarrollar capacidades en otros sectores de la sociedad, así las cosas en las acciones del Plan de Acción y Seguimiento (PAS) del CONPES antes mencionado 1.2, 1.3 y 1.7 del objetivo específico Objetivo 1: Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país, se propone desarrollar el presente proyecto para dar cumplimiento a las metas definidas para la vigencia 2021.

Dicho lo anterior, y teniendo en cuenta lo plasmado en el CONPES antes mencionado el Plan TIC 2018-2022 - el Futuro Digital es de todos, el Ministerio TIC a través de algunas dependencias ha considerado la necesidad de generar programas de formación que contribuyan a la masificación del uso de las herramientas de Seguridad Digital a distintos grupos poblacionales, lo que conlleva cerrar esa brecha existencia y de alguna manera se contina aportando en la transformación digital del país.

La Dirección de Gobierno Digital ha definido e implementado distintas iniciativas tendientes a fortalecer es de las Entidades y de la misma manera contar con se cuenta con los siguientes datos relacionados con las iniciativas definidas por la Dirección de Gobierno Digital y que han permitido obtener un panorama en materia de fortalecimiento de capacidades y la definición de una línea base que permite establecer el impacto conseguido a la fecha.

2.- Descripción del objeto a contratar, con sus especificaciones y la identificación del contrato a celebrar.

2.1. Descripción del Objeto a contratar

2.1.1 Objetivo general:

Dictar cursos certificados en temas relacionados con seguridad de la información, dirigidos a actores del sector público y privado, realizando las convocatorias requeridas para cada grupo objetivo, para lo cual, deberá diseñar y ejecutar una estrategia de formación académica no formal para la vigencia 2021. Así mismo, entregar una propuesta para la estrategia de formación para el año 2022, con el propósito de unificar acciones de generación de capacidades, a través de programas certificados y espacios de sensibilización, entre otros.

2.1.3 Alcance:

El contratista favorecido deberá contar con una oferta académica de cursos certificados, en temáticas relacionadas con Seguridad de la Información descritas en el ítem de

Productos, entregables y resultados esperados. Lo anterior teniendo en cuenta que el público objetivo es el siguiente:

- Profesionales que se desempeñen en entidades públicas a nivel nacional y territorial como gerentes, directores, coordinadores y/o que participen en la toma de decisiones de la Entidad.
- Mujeres interesadas en adquirir conocimientos en seguridad digital, que tengan conocimientos en tecnologías de la Información.

- Estudiantes con formación en áreas relacionadas a tecnologías de la Información o seguridad de la información y afines, con edad entre los 18 a 28 años.

Nota: El contratista deberá realizar por lo menos un (1) curso certificado para cada grupo población.

El contratista deberá garantizar las gestiones que conlleven a que el público objetivo adelante de manera efectiva el proceso de inscripción a las convocatorias.

El contratista deberá realizar el seguimiento a los beneficiarios para que obtengan la certificación de aprobación del curso.

Frente a la propuesta de la estrategia de formación para el 2022, se debe contemplar las actividades de formación y promoción de acuerdo con lo definido en los objetivos estratégicos del CONPES 3995 del 2020.

2.1.4 Elementos o información a tener en cuenta:

- El proveedor seleccionado deberá estar en capacidad de ejecutar el requerimiento de principio a fin, incluyendo los procesos de convocatorias, gestión, control, certificaciones y transferencia del conocimiento.

- El proveedor debe asegurar la plataforma digital para el desarrollo del curso.

- El proveedor debe incorporar el manual de imagen y comunicaciones de MinTIC.

- Los contenidos de la oferta académica propuesta por el proveedor deben ser entregados a AVANCIENCIA para su aprobación, previa validación en conjunto con el MinTIC.

- El diseño de los contenidos de comunicaciones de las convocatorias debe ser entregado a AVANCIENCIA para su aprobación, previa validación en conjunto con el MinTIC.

2.1.5 Entregables:

A continuación, se detallan los productos asociados a la ejecución del contrato:

1. Documento de la estrategia de formación 2022, donde se describa como mínimo los lineamientos, contenidos, actividades y periodo de ejecución de la estrategia de formación para el fortalecimiento de las capacidades en Seguridad de la Información.

2. La oferta académica detallada para cada público objetivo, en temáticas relacionadas con Seguridad Digital tales como:

Para el primer público objetivo:

a. Profesionales que se desempeñen en entidades públicas a nivel nacional y territorial como gerentes, directores, coordinadores y/o que participen en la toma de decisiones de la Entidad.

En temas relacionadas con:

- Seguridad de la Información
- Gestión estratégica de la Seguridad de la Información.
- Seguridad Digital

Duración: 20 horas

Para nuestro segundo público objetivo:

b. Mujeres interesadas en adquirir conocimientos en seguridad digital, que tengan conocimientos en tecnologías de la Información.

En temas relacionadas con:

- Seguridad de la Información
- Gestión de incidentes
- Controles de seguridad y auditoria

Duración: 30 horas

Para nuestro tercer público objetivo:

c. Estudiantes con formación en áreas relacionadas a tecnologías de la Información o seguridad de la información y afines, con edad entre los 18 a 28 años.

En temas relacionadas con:

- Seguridad de la Información
- Conceptos de ciberseguridad
- Gobernanza y gestión de riesgos

Duración: 40 horas

3. Llevar a cabo 3 convocatorias dirigidas al público objetivo que incluyan los requisitos mínimos definidos en este documento y adicionalmente aquellos que el contratista establezca para la realización del curso.

4. Informes de Seguimiento quincenales a las actividades propias del contrato, donde se relacione entre otros, el estado de las convocatorias, el número de certificaciones de asistencia, y certificaciones de aprobación en los casos que aplique, obtenidas por los beneficiarios de las convocatorias.

Nota: Ver los criterios de aceptación del Anexo 6

2.2 Requerimientos específicos que deberá cumplir el proveedor

Características de cada curso:

- Certificaciones expedidas por el contratista.
- La capacitación se realizará de manera 100% en modalidad virtual.
- El contratista dispondrá la plataforma virtual para apoyo en el desarrollo del curso.
- El contratista deberá proveer las herramientas necesarias que permita a los participantes la adecuada realización del curso.
- El plan de estudios deberá contemplar un examen como uno de los requisitos para obtener la certificación de aprobación del curso para el público objetivo de mujeres y jóvenes.
- Definición del porcentaje de participación mínima para obtener el certificado de asistencia.
- Definición del mínimo de participantes necesario para la apertura de cada curso a ofrecer.
- Definición del periodo de tiempo que estará disponible la plataforma para la realización de los cursos.

Convocatorias

El proveedor realizara las convocatorias teniendo en cuenta lo siguiente:

- Definición del cronograma
- Socialización de la convocatoria
- Definición de cupos máximos para el proceso
- Fecha de apertura y cierre
- Condiciones y requisitos para cada convocatoria
- Criterios de selección para cada convocatoria

- Evaluación y publicación de resultados de las convocatorias
- Fecha límite para las inscripciones
- Fecha límite para realizar y culminar cada uno de los cursos
- El número de beneficiarios estará sujeto a la disponibilidad presupuestal

2.3 Especificaciones del contrato

El proveedor deberá entregar un informe de actividades y avance de ejecución del proyecto con una periodicidad semanal, y deberá comprometerse a presentar el cronograma de actividades en un archivo compatible con Microsoft Project.

La generación de las actas de las reuniones de seguimiento serán responsabilidad del proveedor.