Requerimiento Técnico
ELABORACIÓN DE GUÍAS DE SEGURIDAD DIGITAL PARA LA 4RI

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

El Gobierno Nacional ha establecido dentro del Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la equidad" bajo el fundamento de Legalidad, los objetivos de:

- Proporcionar una política de Estado para la transformación digital y el aprovechamiento de la cuarta revolución industrial, a través de la interoperabilidad de plataformas, contacto a través del Portal Único del Estado, uso de tecnologías emergentes, seguridad digital, formación en talento digital, y fomento del ecosistema de emprendimiento.

- Uso Big Data en la lucha contra la corrupción.

Para dar alcance a estos objetivos planteados y en concordancia con el CONPES 3995 de 2020 "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL" específicamente en desarrollo del objetivo específico 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 4RI, más específicamente las acciones del PAS del CONPES 3.2 y 3.3 que define el vehículo de cumplimiento de dicho objetivo de la política.

Lo anterior es necesario como herramienta y guía para la implementación en las entidades, dado que se incrementaron en un 300 % en el primer semestre de 2019 los ataque a IoT y si se tiene en cuenta que actualmente existen casi 21 billones de dichos dispositivos en el mundo, el riesgo de ataques es alarmante. Ahora bien, si para 2025 se espera que la cifra de dichos dispositivos se duplique (Foro Económico Mundial, 2020).
Teniendo en cuenta lo anterior el grupo de seguridad y privacidad de la información coherente con el desarrollo de lineamientos para mejorar los niveles de seguridad en el país y en concordancia con los requerimientos generados a través del CONPES 3995 de 2020 referentes a las tecnologías emergentes se pretende cerrar las brechas de seguridad a través del establecimiento de mejores prácticas para:

- Internet de las cosas (IoT)

- Big data
- Computación en la Nube
- Inteligencia Artificial (IA).
- Blockchain
- Obsolescencia tecnológica.

Para tal fin se realizarán guías para la implementación, uso y manejo para la gestión de los riesgos de seguridad digital en las entidades públicas del país teniendo como estrategia el involucramiento de las múltiples partes interesadas (entidades públicas, privadas, Academia y sociedad civil), por lo cual se realizará en las siguientes fases:

1. Creación de las guías a través de la entidad contratada. Siendo supervisada su realización a través del equipo de seguridad y privacidad de la Subdirección de Estándares y Arquitectura de la Dirección de Gobierno Digital.
2. Establecer el periodo de consideraciones para las entidades públicas, privadas y sociedad civil.
3. Realizar mesas de trabajo con la academia y someter a discusión las opiniones generadas por las demás partes interesadas.
4. Generar el modelo acorde a las recomendaciones de las partes interesadas.

El anterior planteamiento se basa en lo establecido en el CONPES 3995 de 2020 en el marco de los principios fundamentales de la política de Confianza y Seguridad Digital, en particular la salvaguarda de los derechos humanos, así como del derecho internacional humanitario.

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:

Generar guías orientadas al uso de tecnologías emergentes y la actualización tecnológica de las entidades del Estado, teniendo en cuenta lineamientos para la gestión de los

riesgos de seguridad digital, de tal forma que apoyen en la preparación del país hacia los desafíos de la 4RI, a través de la generación de buenas prácticas alineadas a los marcos internacionales y mejores prácticas de seguridad digital.

2.1.2 Objetivos específicos:

1. Crear cinco (5) guías metodológicas para la identificación y gestión de riesgos de seguridad digital en la adopción de tecnologías de la cuarta revolución industrial, tales como, Internet de las cosas (IoT), Blockchain Big data, Computación en la Nube, Inteligencia Artificial (IA).

2. Desarrollar una (1) guía que contenga lineamientos y acciones para la adopción y actualización de tecnologías para las entidades públicas, con el fin de disminuir las vulnerabilidades derivadas de la obsolescencia tecnológica.

2.1.3 Alcance:

El servicio de generación de cada una de las guías metodológicas debe comprender las siguientes fases:

- Levantamiento de información previo al desarrollo de las guías, enfocado a determinar los incidentes de seguridad en las entidades públicas, el cual deberá cumplir con los siguientes entregables: definición de la población objeto del estudio, creación y validación del instrumento y resultados de la aplicación con los respectivos análisis cuantitativos que dé a lugar.

- Generar guías metodológicas (5) para las tecnologías emergentes para la gestión de los riesgos de seguridad digital y obsolescencia tecnológica

- Adoptar las recomendaciones obtenidas de las partes interesadas durante el periodo de comentarios.

- Los datos recolectados deberán tener una metodología previamente establecida y deben ser documentadas previo análisis cuantitativo o cualitativo de acuerdo con la metodología seleccionada.

- Socializar con las entidades del orden Nacional y Territorial a través de sesiones en línea, que permita generar las capacidades necesarias con los encargados de ciberseguridad y CIO’s para la reducción de los riesgos en los desarrollos e implementaciones enfocados a las tecnologías emergentes y obsolescencia tecnológicas.

- Dar cumplimiento a lo establecido en las metas 3.2 y 3.3 CONPES 3995 de 2020.

-

2.1.4 Elementos o información a tener en cuenta:

Dichos lineamientos y guías se integrarán a la actual política de Gobierno Digital y se enmarcarán en los principios establecidos en el Artículo 147 de la Ley 1955 de 2019 por la cual se expide el Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad”.

2.1.4 Entregables:

Los entregables se relacionan a continuación:

1. Generar guías metodológicas para la gestión de los riesgos de seguridad digital de las tecnologías emergentes las cuales deben contener como mínimo:

    - Los antecedentes de cada una de las tecnologías.
    - Clasificación de las herramientas o elementos disponibles.
    - Establecer el contexto de uso y beneficios.
    - Marco regulatorio.
    - Gobierno abierto (transparencia, colaboración, participación, desarrollo de capacidades
    - Ejemplos de implementación a nivel global.
    - Posibles procesos de implementación de estas tecnologías a nivel Colombia.
    - Esquemas y procesos de implementación.
    - Buenas prácticas y principios para la adecuada implementación de estas tecnologías en entidades públicas.
    - Herramienta para identificación de necesidad y aplicabilidad de proyectos basados en tecnologías emergentes.
    - Gestión de riesgos.
    - Mejora continua.
    - Recomendaciones.

2. Generar guía metodológica para la gestión de los riesgos de seguridad digital de la obsolescencia tecnológica, la cual debe contener como mínimo:

    - Situación en el Sistema Nacional de Salud respecto a RAEE's y RESPEL.
    - Perfil tecnológico.
    - Referencias internacionales sobre la gestión de los ciclos de vida de la tecnología.
    - Marco legal Nacional.
    - Proceso de eliminación segura de datos.
    - Riesgos de seguridad.
    - Eliminación segura y reciclaje tecnológico.
    - Gestión de riesgos.
    - Mejora continua.
    - Recomendaciones.

Nota: Ver los criterios de aceptación del Anexo 6

2.2 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.