AGENDA ESTRATÉGICA DE INNOVACIÓN: CIBERSEGURIDAD

Bogotá D.C., Marzo de 2014

AGENDA ESTRATÉGICA DE INNOVACIÓN: CIBERSEGURIDAD

SISTEMA DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN
SUBSISTEMA DE INNOVACIÓN PARA EL USO Y APROPIACIÓN DE TIC EN EL GOBIERNO

Bogotá D.C., Marzo de 2014

Ministerio de Tecnologías de la Información y las Comunicaciones

AGENDA ESTRATÉGICA DE INNOVACIÓN: CIBERSEGURIDAD

Plan Vive Digital:

Hugo Sin Triana – Líder I+D+i

Con la colaboración de CINTEL.

TABLA DE CONTENIDO

1. CIBERSEGURIDAD

Las Tecnologías de la Información y las Comunicaciones, por su característica transversal, se han convertido en el principal vehículo de la sociedad de la información, el soporte fundamental de las estructuras organizacionales y uno de los elementos angulares dentro de las actividades principales de todos los sectores económicos del país. Esta posición ha convertido a las TIC en un activo estratégico dentro de las políticas nacionales e internacionales, y por tal motivo ha hecho visible la necesidad de establecer mecanismos que permitan controlar el uso adecuado de este activo, pues su afectación tendría un serio impacto social, político y económico.

Las Tecnologías de la Información y las Comunicaciones se han involucrado en todos los eslabones de la sociedad moderna, desde las organizaciones públicas y privadas, que cada día se esfuerzan más por incorporar TIC en sus procesos, buscando así impulsar la optimización de tiempos y de recursos, la reducción de costos y la agilización en sus procesos; hasta el ciudadano, a través de la computación móvil, los teléfonos inteligentes, las iniciativas nacionales para facilitar el acceso a computadores y conectividad de Internet, y la creciente dependencia a la tecnología. Este nuevo esquema ha configurado una sociedad donde la información es el activo principal, donde el concepto de ciberespacio ha adquirido dimensiones estratégicas, y donde el cuidado de recursos y activos informáticos se ha constituido en un foco fundamental.

La información, apalancada por la velocidad, la capacidad y el acceso que brindan las TIC, se ha visto enfrentada a un nuevo panorama de riesgos donde las amenazas son ahora de naturaleza cibernética, donde los intangibles son críticos para el funcionamiento de las organizaciones y la sociedad en general, y donde los impactos de la materialización de los riesgos siguen siendo reales. Este esquema ha demostrado que los estados requieren plantear estrategias e iniciativas que minimicen la posibilidad de que estos nuevos riesgos se hagan efectivos, que eviten que los ciudadanos, los sectores productivos y el Estado en general se vean afectados, y que con esto se altere la forma de organización social, económica, política soberana y coercitiva del país.

Para esto, Colombia ha empezado a plantear una visión rectora consolidada en el documento CONPES 3701, el cual busca generar los lineamientos nacionales de política en ciberseguridad orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. En este marco de referencia se define la ciberseguridad como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado y a la ciudadanía en general ante estas nuevas amenazas. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países y Colombia no es la excepción, dado

que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil.

En este contexto, la política criminal definida por la Corte Constitucional Colombiana en varios pronunciamientos, en especial, aquel contenido en la sentencia C-936-10, la misma es entendida como “el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción”. La jurisprudencia constitucional ha reconocido así mismo que la política criminal puede ser articulada por el Legislador a través de la expedición de normas. En este sentido indicó que: “la legislación penal es manifestación concreta de la política criminal del Estado”, y que “la decisión política que determina los objetivos del sistema penal y la adecuada aplicación de los medios legales para luchar contra el crimen y alcanzar los mejores resultados, se plasma en el texto de la ley penal”.

Así mismo, se precisó que “la norma penal, una vez promulgada, se independiza de la decisión política que le da origen, conservando la finalidad buscada por su redactor en el elemento teleológico de la norma”; lo que cobra especial significación, a efectos de alinearse con las políticas públicas de ciberseguridad con miras a reducir, prever y remediar la vulneración a los derechos constitucionales y legales comprometidos por el uso ilegítimo de las Tecnologías de la Información y las Comunicaciones.

Los vectores de desarrollo que aquí se presentan corresponden a directrices marco que se han identificado como prioritarias para Colombia, orientadas a fortalecer la posición del país en términos de ciberseguridad, alineados con las diferentes estrategias y normativas nacionales provenientes desde las entidades del Estado y del sector privado, y que con su fortalecimiento conlleven a mejorar la posición estratégica del país en estos temas. Cada uno de estos vectores está compuesto por líneas temáticas, las que detallan los temas específicos en los cuales se debe enfocar los esfuerzos de innovación en el país.

2. VECTORES DE DESARROLLO

A continuación se presentan los vectores de desarrollo que enmarcan las actividades de innovación alrededor de la temática de ciberseguridad.

2.1 Principios rectores de Ciberseguridad

Diferentes países alrededor del mundo han establecido como una de sus estrategias fundamentales el planteamiento de alternativas metodológicas desarrolladas en términos de políticas, normas, procedimientos, estándares y de la definición de niveles específicos de referencia en términos de ciberseguridad que se encuentren alineados con las diferentes estrategias nacionales, con los desarrollos normativos particulares y con las directrices planteadas a través de Ministerios, Unidades Administrativas y Programas nacionales, así como también con legislación internacional, con directrices dadas por los organismos de normalización y estandarización y con políticas establecidas por las diferentes asociaciones internacionales, todo con el fin de fortalecer la posición estratégica del Estado en el ciberespacio y enfrentar de manera adecuada los riesgos de naturaleza cibernética a los que se ve expuesto.

El objetivo principal de esta estrategia es orientar todos los esfuerzos nacionales, desde un enfoque estratégico, para fortalecer la posición de estos países en términos de aseguramiento de su infraestructura crítica, de protección de los servicios que proveen a sus ciudadanos y de todos los sistemas y activos sobre los que soportan la operación de las entidades del Estado, así como también el establecimiento de una ventaja competitiva en términos de defensa estratégica del ciberespacio y de las Tecnologías de la Información y las Comunicaciones con las que se soportan todas las actividades y procesos del Estado. Este planteamiento estratégico se materializa, de manera particular, mediante la creación de guías rectoras, a nivel de regulación y legislación, que especifican de forma puntual y detallada las medidas requeridas para aumentar la seguridad de los sistemas y activos de información que se manejan en los respectivos gobiernos, las cuales deben ser estructuradas de manera conjunta por los diferentes actores de la sociedad para garantizar así su viabilidad y su factibilidad tecnológica, ajustada y alineada con la realidad tecnológica del estado particular de implementación, así como también su pertinencia política y social.

Ante este entorno, se plantea un escenario en el que es posible y necesario complementar y fortalecer el trabajo que se ha empezado a elaborar en Colombia, especialmente el realizado por el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Programa Gobierno en Línea, que ha avanzado enormemente en términos de políticas, procedimientos, controles y recomendaciones técnicas para el fortalecimiento de la ciberseguridad del Estado, buscando así cerrar la brecha existente en términos de políticas de prevención, de control y de reacción ante el incremento constante de amenazas informáticas, la ausencia de guías tecnológicas específicas y la heterogeneidad de medidas que se buscan aplicar a las instituciones del Estado colombiano.

De esta forma, es necesario que los diferentes actores de la sociedad, la Academia, la Empresa y el Gobierno, orienten esfuerzos a la generación de proyectos, iniciativas y planteamientos innovadores de política y normatividad pública enfocados en fortalecer la posición del país en términos de gestión de seguridad de la información, definición y aseguramiento de infraestructura crítica, el mantenimiento de ambientes seguros, el aseguramiento de sistemas y la definición de niveles mínimos suficientes para controlar los riesgos y amenazas de naturaleza cibernética, así como las medidas estratégicas para la gestión de la ciberseguridad, y la configuración de un entorno político adecuado para la implementación de medidas para asegurar al Estado en el ciberespacio, pues es necesario apalancar estas nuevas necesidades desde el punto de vista legislativo, donde los mecanismos de control y de vigilancia son fundamentales para garantizar la estabilidad de las instituciones y la consecución de los objetivos estratégicos del Estado, potenciando así la transparencia, la oportunidad, y la optimización de recursos.

Las innovaciones en este vector de desarrollo se deben enmarcar en una o varias de las siguientes líneas temáticas:

A. Generación de políticas, directrices, normas, actos administrativos y otras formas jurídicas que dictaminen las formas, tanto tecnológicas como procedimentales, de llevar a cabo el intercambio de información entre las diferentes entidades del Estado, entre el Gobierno y los diferentes sectores productivos del país y entre la ciudadanía en general, bajo esquemas que garanticen la integridad, la confidencialidad y la disponibilidad de la información.

B. Generación de políticas, normas, actos administrativos, procedimientos legislativos y otras figuras jurídicas orientadas a fortalecer las capacidades y la organización del Estado colombiano para proteger al ciberespacio de amenazas que atenten contra la soberanía nacional y los principios constitucionales.

C. Incorporación de los delitos cibernéticos como elemento fundamental de las políticas, normas, actos administrativos y otras figuras jurídicas, con el fin de fortalecer al Estado en su capacidad para identificar, reconocer y juzgar de manera adecuada estos elementos en los procesos jurídicos, constitucionales, penales, etc., definiendo también los alcances, los niveles de gravedad, las penalidades y los procedimientos necesarios ante la ocurrencia de los mismos.

D. Generación de directrices de protección de la confidencialidad, integridad y disponibilidad de los datos del Estado Colombiano durante el ciclo de vida de los mismos, a través de la definición, adopción, ajuste, actualización, incorporación, implementación y valoración de esquemas tecnológicos y procedimentales específicos.

E. Dimensionamiento de políticas de seguridad de la información y ciberseguridad para la incorporación de software en las entidades del Estado, así como para su gestión, dirección, monitoreo, mantenimiento y control, considerando esquemas técnicos, procedimentales, metodológicos y de política nacional.

F. Generación de políticas, normas, actos administrativos, procedimientos legislativos y otras figuras jurídicas orientadas a fortalecer las alianzas y los acuerdos de cooperación y colaboración internacionales de lucha contra amenazas y delitos de naturaleza cibernética, así como aquellos orientados a fortalecer la defensa nacional en el ciberespacio.

G. Estructuración de circulares, políticas, normas, actos administrativos y otras figuras enfocadas a fortalecer las capacidades del Estado para garantizar la adecuada identificación/autenticación, autorización de los ciudadanos colombianos, así como protección de la identidad de los mismos.

Es importante resaltar que todos los elementos de innovación deben considerar en su estructuración los resultados que surjan desde las entidades que tienen obligaciones específicas en términos de Ciberseguridad, según lo definido en el CONPES 3701, tales como los resultados de las iniciativas planteadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, el Ministerio de Relaciones Exteriores, la Fiscalía General de la Nación y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, entre otros.

2.2 Educación, formación y divulgación en Ciberseguridad

Uno de los factores fundamentales para garantizar un adecuado conocimiento y desenvolvimiento de los funcionarios públicos, y de la sociedad en general, en temas relacionados con ciberseguridad, radica en la educación y formación de calidad y de alto nivel del recurso humano quien, como ente activo que produce, consume y transforma información, se configura como el eslabón más débil de la cadena de seguridad de la información del Estado. Esta situación se convierte en la razón fundamental para impulsar estrategias orientadas a generar una conciencia de la responsabilidad y una obligación específica de salvaguardar la información como activo fundamental en la sociedad del conocimiento.

Esta nueva responsabilidad recae ante cualquier individuo que forma parte del recurso humano de una institución, que recibe los recursos técnicos y de información, como insumo indispensable para la ejecución de sus funciones laborales, bien sean misionales, de apoyo o estratégicas y que, independiente a la profesión, cargo, funciones o tiempo de servicios prestados a la institución, debe responder con ética y principios sobre la integridad, veracidad, confidencialidad y disponibilidad de la información, así como del uso que se le da a la misma. Es por esto que se vuelve fundamental, poner a disposición de la comunidad en general, las herramientas metodológicas y conceptuales que permitan una preparación cognitiva y psicológica para responder apropiadamente ante un incidente de naturaleza cibernética que ponga en riesgo la información del Estado en general, y del ciudadano en particular.

Alrededor del mundo se han generado múltiples iniciativas en este sentido, formalizando los esquemas educativos a través de certificaciones con reconocimiento internacional, programas educativos técnicos y tecnológicos, y programas profesionales de pregrado y posgrado. Esto impulsado por la creciente necesidad de contar con personal altamente capacitado y calificado en temas de ciberseguridad que tengan las capacidades suficientes para afrontar todo el conjunto de nuevos retos que se presentan ante la sociedad de la información, donde el ciberespacio y las tecnologías digitales se convierten en las nuevas

herramientas de trabajo, configurando una sociedad totalmente dependiente de las Tecnologías de la Información y las Comunicaciones, situación que cambia radicalmente el panorama habitual de riesgos. Así mismo, este nuevo esquema implica un esfuerzo en realizar actividades de divulgación sobre los avances y oportunidades que se presentan a lo largo de la cadena de valor de la ciberseguridad, el cual debe estar enfocado a todos los sectores de la sociedad.

En este sentido, es necesario establecer estrategias de amplio espectro y profundo impacto con el fin de alinear a los funcionarios públicos y a la sociedad en general ante este nuevo entorno, en el cual la información se convierte en el activo más importante y donde es necesario tomar medidas de protección y de control que no son necesarias en otros ámbitos. Iniciativas que permitan la dinamización de los espacios de estructuración, coordinación y establecimiento de “think tanks”, grupos de discusión y equipos de trabajo orientados a temáticas específicas de seguridad de la información y ciberseguridad.

Teniendo en cuenta esta nueva complejidad, se vuelve imperativo establecer proyectos de innovación en las siguientes líneas temáticas:

A. Establecimiento, estructuración, diseño e implementación de programas de formación técnica, tecnológica y profesional de alto nivel y de calidad internacional, pensum académicos y syllabus curriculares en temas técnicos y legales de seguridad de la información y ciberseguridad.

B. Definición, adopción, estructuración, implementación y prueba de esquemas metodológicos, pedagógicos y educativos de buenas prácticas en seguridad de la información para las entidades del Estado y con las que estas interactúen, así como de modelos de enseñanza e incorporación de conocimiento, competencias y habilidades en seguridad de la información y ciberseguridad.

C. Análisis, diseño, estructuración, implementación y evaluación de estrategias de sensibilización y apropiación orientadas a la comunidad en general, por sectores políticos, socioeconómicos, culturales y educativos.

Es importante resaltar que todos los elementos de innovación que se planteen a través de estas líneas temáticas, deben considerar los resultados de las estrategias y políticas definidas por el Ministerio de Educación Nacional y del Programa Gobierno en Línea.

2.3 Gestión integrada de riesgos e incidentes de naturaleza cibernética

Un elemento fundamental para la adecuada aproximación hacia un Estado con niveles apropiados de ciberseguridad requiere un enfoque estructurado para la gestión y el manejo de los riesgos y amenazas asociadas a los sistemas y activos de información de todas las entidades, por esta razón se ha observado la necesidad de establecer procesos formales que permitan mantener un panorama continuo de la seguridad de la información, de las amenazas y vulnerabilidades, y de los diferentes elementos de naturaleza cibernética que interactúan dentro de las entidades y entre ellas, con el fin de agilizar el proceso de toma de decisiones para la gestión de los riesgos y de incidentes.

En Colombia se han establecido los lineamientos básicos para el establecimiento organizativo de la respuesta del Estado ante los riesgos e incidentes de naturaleza cibernética, lo que ha puesto a consideración la necesidad de contar con esquemas, modelos, procesos y herramientas que permitan la captura de datos, el análisis, el transporte y la respuesta, de manera integrada, ante este tipo de situaciones. Esto ha impulsado la necesidad de que en el país se realicen procesos de innovación orientados a la generación de soluciones en Tecnologías de la Información y las Comunicaciones que estén en capacidad de buscar, identificar, estructurar, analizar, recuperar, correlacionar y/o integrar datos relacionados con las incidencias de naturaleza cibernética, que se presenten a lo largo del país, en las regiones, o en entidades particulares, fomentando la interoperabilidad y el intercambio de datos a través de esquemas desagregados, que le brinden al país en general y a las entidades en particular la capacidad de responder, prevenir y evitar estos eventos y mantener un efecto disuasivo estratégico.

En este orden de ideas, se hace necesario plantear estrategias nacionales concertadas en torno a las dificultades y necesidades expeditas en términos de ciberseguridad, en las cuales se deberán trabajar de manera complementaria la estructuración y puesta en marcha de esquemas tecnológicos de gestión continua que permitan detectar y tratar apropiadamente los riesgos de ciberseguridad, y el establecimiento e implementación de arquitecturas de seguridad que faciliten los procesos de estandarización y medición de los niveles de riesgos y de incidentes, de forma tal que se pueda brindar un cuadro generalizado de indicadores, que sean comparables entre las diferentes entidades, que se puedan estructurar mediante estrategias de federación, y que permitan identificar de manera adecuada la situación nacional en términos de riesgos e incidentes de naturaleza cibernética, brindando un enfoque común entre los diferentes actores nacionales, independientemente de su sector, tamaño o responsabilidades específicas.

Para responder a los retos modernos, teniendo en cuenta la complejidad tecnológica asociada y la gran variedad de entidades que conforman al Estado colombiano, se estructuran las siguientes líneas temáticas:

A. Estructuración, diseño, desarrollo e implementación de modelos distribuidos (federados) para la medición (preferiblemente automatizada, continua y en tiempo real) de los mapas de riesgos, amenazas y vulnerabilidades existentes en los sistemas de información del Gobierno, para entidades individuales y que permitan la medición comparable por grupos de entidades (por ejemplo, sectores productivos), facilitando la toma de decisiones en cuanto a prevención, protección y detección temprana de incidentes.

B. Estructuración, diseño, desarrollo e implementación de modelos para la gestión federada de incidentes, orientadas al diseño, adaptación, desarrollo, establecimiento y puesta en funcionamiento de sistemas integrados que permitan monitorear, detectar, prevenir, informar, responder, alertar de manera temprana y tratar de forma apropiada incidentes de naturaleza cibernética.

C. Estructuración e implementación de modelos, tecnologías y controles operativos para el uso de activos críticos y de recursos tecnológicos del Estado colombiano, así como para la incorporación de

nuevos recursos y la disposición de aquellos que salen de servicio, con el fin de minimizar riesgos asociados al transporte, procesamiento y almacenamiento de información crítica.

D. Estructuración y definición de esquemas tecnológicos y metodológicos de modelado y simulación de riesgos cibernéticos que permitan identificar de manera temprana los riesgos de naturaleza cibernética a las que está expuesto el Estado colombiano, y que le brinden al Estado la capacidad preventiva y reactiva ante incidentes.

E. Definición, adopción, estructuración, coordinación, formación, entrenamiento, conformación e implementación de centros y equipos de respuesta a incidentes, tanto a nivel nacional como a nivel regional y local, por sectores económicos, que estén en articulación con las iniciativas y esfuerzos planteados desde el ColCERT y el CSIRT de Colombia.

Es importante resaltar que todos los elementos de innovación que surjan en torno a estas líneas temáticas deben considerar en su estructuración los resultados de las estrategias y políticas definidas en términos de gestión de riesgos por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT.

2.4 Identificación, autenticación y autorización

El Estado colombiano ha establecido múltiples iniciativas tendientes a unificar los mecanismos de identificación de la ciudadanía colombiana, incorporando así dentro del proceso tecnología de punta para tal fin, sin embargo, todos estos esfuerzos aún no han sido suficientes para garantizar que el Estado cuente con mecanismos generalizados, estandarizados, robustos y homogéneos que le permita llevar un registro sobre sus ciudadanos, en aras de proteger sus derechos y libertades constitucionales, de manera transversal a todas las entidades, instituciones y empresas. Esta situación se ve también reflejada en la aparición de esquemas individualizados de identificación en el sector privado, generando así re-procesos y cargas administrativas adicionales, que se podrían minimizar mediante la innovación en modelos, esquemas, mecanismos, herramientas y sistemas que permitan una gestión unificada de la identidad de los ciudadanos colombianos, en términos de autorización y autenticación.

Con el fin de dar respuesta a esta situación, es necesario plantear esquemas innovadores orientados sobre las siguientes líneas temáticas:

A. Definición y estructuración de modelos, esquemas técnicos, procedimentales y metodológicos para la identificación/autenticación ciudadana, los cuales permitan la gestión integrada de identidad para el acceso a servicios, en particular aquellos servicios que se prestan por Internet y para la protección de identidad, con base en modelos y experiencias exitosas registradas en otros países.

B. El establecimiento, diseño, estructuración, incorporación, implementación y valoración de esquemas tecnológicos y procedimentales para garantizar la identificación, autenticación y autorización de funcionarios, ciudadanos, activos de información y recursos que acceden a la infraestructura del

Estado colombiano, mediante la generación de modelos y esquemas de autenticación de múltiple factor.

Así mismo, es necesario que estos esquemas contemplen las iniciativas presentadas por la Registraduría Nacional del Estado Civil, por el Programa Gobierno en Línea y aquellas iniciativas puntuales de identificación y registro planteados por los organismos de seguridad del Estado.

2.5 Aseguramiento de aplicaciones y ambientes móviles en el Gobierno

Uno de los sectores de mayor dinámica en la economía global es el relacionado con el desarrollo de software y de aplicaciones móviles, el cual, dado el auge de dispositivos electrónicos, la masificación del acceso a Internet y la capacidad resultante que brinda el ciberespacio para comunicarse a través de las redes de datos y de compartir información en tiempo real (característica propia de la actual sociedad del conocimiento), se ha convertido en uno de los sectores más críticos y delicados dentro del ecosistema de la ciberseguridad, lo que lo ha llevado a ser un sector pionero, con inversiones considerables, con una proyección acelerada y que genera un mayor interés por parte de la población en general, de los actores políticos y de los organismos de seguridad y defensa del Estado.

Este sector, en los últimos años, se ha caracterizado por brindar el soporte fundamental para que las personas interactúen y disfruten de las ventajas presentadas por las Tecnologías de la Información y las Comunicaciones, configurando espacios en los cuales puedan interactuar con sus semejantes o con las entidades del Gobierno, permitiéndole hacer uso de los servicios que éstas ponen a disposición de la ciudadanía, y fortaleciendo los resultados de iniciativas como las establecidas por el Programa Gobierno en Línea.

Esta situación ha tenido un éxito tal que ha permeado todas las capas de la sociedad, sumergiéndola en toda una plataforma tecnológica con innumerables posibilidades. Esta plataforma, sin embargo, también representa un reto adicional en términos tecnológicos y de gobierno, en la cual se hace necesario establecer y definir un conjunto de responsabilidades adicionales en torno a la necesidad de proteger los datos, la información y los dispositivos que interactúan dentro de este nuevo esquema, para así brindar confianza en el uso de los nuevos servicios, y poder facilitar la interacción entre los ciudadanos y de estos con el Gobierno en general.

De esta forma, para garantizar que todo este conjunto de nuevas interacciones se realicen de manera segura, siguiendo directrices apalancadas en la protección a la ciudadanía y manteniendo al Estado dentro de los límites establecidos de ciberseguridad, se hace necesario establecer esquemas innovadores en las siguientes líneas temáticas:

A. Definición y estructuración de metodologías para la implementación del Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea, para el aseguramiento de la elaboración, desarrollo, seguimiento y sostenibilidad del Sistema de Gestión de Seguridad de la Información en las entidades del Estado.

B. Definición, adopción, ajuste, actualización, incorporación, implementación y valoración de modelos de desarrollo de software *in-house* orientados a suplir las necesidades de seguridad de información en las entidades colombianas, que estén apalancados en estándares internacionales y que se ajusten a las mejores prácticas internacionales en la materia.

C. Definición, adopción, estructuración e implementación de metodologías estándar unificadas, ajustadas al entorno colombiano, para el aseguramiento de la información y del software en los dispositivos móviles que están en uso en las entidades del Estado y para aquellos que estén próximos a adquirirse.

D. Definición, adopción, estructuración e implementación de metodologías, procedimientos y estrategias generales para el control de acceso a la información y a contenidos en las entidades del Estado y en sectores específicos (p.ej. el sector educativo), los cuales se deben articular desde todas las etapas del ciclo de desarrollo de software y de tecnología específicos.

E. Establecimiento, estructuración, diseño e implementación de modelos, esquemas tecnológicos, procedimentales y metodológicos para el aseguramiento de la información en las diferentes etapas de los ciclos de desarrollo de aplicaciones que son utilizadas en las instalaciones de Gobierno, para prestar servicios a la ciudadanía, al Gobierno mismo y al sector privado, o que sean de misión crítica.

F. Establecimiento, estructuración, diseño e implementación de modelos, esquemas y soluciones tecnológicos, procedimentales y metodológicos para el aseguramiento de la infraestructura tecnológica que presta servicios a la ciudadanía y utilizada por la población general (cibercafés, cafés Internet, telecentros, salas públicas, etc.) que propendan por la oferta de servicios seguros de acceso a Internet.

Es importante resaltar que todos los elementos de innovación que surjan en torno a estas líneas temáticas deben considerar los resultados de las estrategias y políticas definidas en términos de desarrollo de aplicaciones por el Ministerio de Tecnologías de la Información y las Comunicaciones, por el Ministerio de Defensa Nacional, el Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT y los organismos de normalización y estandarización con reconocimiento en el ámbito colombiano.

2.6 Tecnologías de la Información y las Comunicaciones para el Sector Defensa

Sin prejuicio de las temáticas anteriormente mencionadas, se hace necesario fortalecer e impulsar programas, políticas, proyectos y desarrollos específicos dentro de las instituciones encargadas de mantener la seguridad y defender la soberanía del Estado colombiano en el ciberespacio, con el fin de configurar una ventaja estratégica, operativa y táctica sobre la inherente asimetría existente en cuanto a ciberseguridad.

Es de especial importancia el planteamiento de esquemas innovadores, tanto a nivel de tecnologías, como de metodologías y procedimientos que le permitan al Estado anteponerse a los riesgos que surgen a diario en el ciberespacio, o que son inherentes al uso de Tecnologías de la Información y las Comunicaciones para apalancar las actividades realizadas por los organismos de seguridad del Estado y que, ante la materialización de riesgos, la explotación de vulnerabilidades o el aprovechamiento de debilidades, representan un elemento desestabilizante para la soberanía del Estado, la seguridad de los ciudadanos, y los intereses del sector público y privado.

Dentro de este contexto es importante desarrollar iniciativas innovadoras en las siguientes líneas temáticas:

A. Definición y estructuración de esquemas tecnológicos y metodológicos para garantizarle al Estado colombiano una ventaja táctica y estratégica en el ciberespacio, a partir de la identificación, perfilación, monitoreo y control de la infraestructura crítica del país, entendida ésta como todos los elementos de infraestructura nacional que están expuestos a riesgos de naturaleza cibernética y que, ante la eventualidad de un incidente pueden generar un impacto catastrófico en la política, economía, sociedad y soberanía del Estado colombiano.

B. La definición, adopción, ajuste, actualización, incorporación, implementación y valoración de tecnologías específicas de defensa y ataque cibernético que debería considerar el Estado colombiano para fortalecer su posición en términos de ciberseguridad, para proteger su soberanía y para brindarle herramientas que le permitan cumplir con los deberes definidos constitucionalmente y salvaguardar los derechos de la ciudadanía.

C. Definición, estructuración y diseño de estudios sectoriales que le permitan al Estado colombiano identificar de manera temprana las necesidades de innovación en temas de ciberseguridad, y que le permitan anteponerse a los riesgos, tendencias y problemáticas que estén surgiendo en esta materia.

Es claro que muchos de estos esquemas, dada su criticidad y su importancia a nivel estratégico para el Estado colombiano, son de carácter confidencial y reservado.