MARCO DE GOBIERNO Y GESTIÓN DE CIBERSEGURIDAD PARA CIUDADES INTELIGENTES EN EL CONTEXTO COLOMBIANO

CASO DE ESTUDIO: CIUDADES COLOMBIANAS DE CATEGORÍA I Y II

Preparado por:

Ing. Geovanna Patricia Peña Barranco

Asesores:

Lucy Esther García Ramos

Wilson Nieto Bernal

UNIVERSIDAD DEL NORTE

División de Ingenierías

Departamento de Ingeniería de Sistemas

Maestría en Gobierno de Tecnología Informática

Barranquilla, Colombia

2021

DEDICATORIA

A Dios por la vida y la salud.
A mis padres Luis y Maribel, a mi hermana Eyleen por su amor, enseñanzas, confianza y apoyo incondicional siempre.
A Javier por su amor y compañía.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

1. TITULO

MARCO DE GOBIERNO Y GESTIÓN DE CIBERSEGURIDAD PARA CIUDADES INTELIGENTES EN EL CONTEXTO COLOMBIANO

Caso de estudio: Ciudades Colombianas de categoría I y II

2. INTRODUCCIÓN

Durante las últimas décadas hemos presenciado dos acontecimientos importantes para la humanidad: la cuarta revolución industrial (o tecnologías 4.0) y el crecimiento de la urbanización a nivel mundial. Es tanto este crecimiento que la Organización de las Naciones Unidas (ONU), calcula que actualmente más de la mitad de la población mundial vive en ciudades y para el 2050, será del 68% de la población.

En el año 2015 los lideres mundiales se reunieron y plantearon 17 Objetivos de Desarrollo Sostenibles (ODS) que se espera estén cubiertos en el año 2030. las ciudades son vistas como el núcleo de estas estrategias y las nuevas tecnologías aportarán no solo al cumplimiento del objetivo once, “Ciudades y comunidades sostenibles”, sino a la consecución de la mayoría de los objetivos. En términos generales los ODS han sido un motor para impulsar la revolución de las ciudades (ONU, 2018).

Estas “nuevas ciudades” que integran las tecnologías de la cuarta revolución industrial, permiten recopilar datos y con su análisis tomar mejores decisiones para la sostenibilidad y la prestación de servicios al ciudadano. Sin embargo, estas tecnologías son susceptibles y objetivos constantes de ciberataques. Por tanto, es necesario realizar una correcta planeación, especialmente en asegurar la integridad de los datos y evitar ciberataques que atenten contra la infraestructura y continuidad de los servicios.

3. DESCRIPCIÓN DEL PROBLEMA

Durante las últimas décadas en todo el mundo se ha presentado un incremento significativo de la población de las áreas urbanas. De acuerdo con proyecciones de la ONU para el año 2050 el 68% de la población mundial vivirá en las ciudades, este incremento se prevé debido a que las personas continúan mudándose desde las áreas rurales en búsqueda de mejores oportunidades, se ha presentado un aumento en la longevidad de la población y un incremento general de la población mundial, esto se traducirá en aproximadamente 2500 millones de personas viviendo en las urbes (ONU, 2018).

Colombia no es ajena a este fenómeno, Miguel Ángel Cárdenas Contreras director de Geoestadística del DANE, en su análisis sobre crecimiento urbano en Colombia, resaltó que en los últimos 20 años la población en las cabeceras municipales se ha incrementado en un 37,2% lo que genera en sí mismo una necesidad de cobertura de servicios a muchísimos habitantes tanto actuales como futuros (IEU,2017). Esta situación trae consigo una serie de retos asociados a la prestación de servicios públicos, manejo de desechos, cambio climático, consumo de recursos naturales, transporte, productividad, sostenibilidad, seguridad ciudadana, educación, vivienda, equidad e inclusión social y por tanto un aumento en la demanda de más y mejores servicios que buscan repercutir en la calidad de vida de los ciudadanos.

Desde el sector público se han trazado planes y políticas que buscan dar respuesta a esta situación maximizando la oferta de servicios públicos y privados que no vayan en detrimento de los cada vez más escasos recursos naturales, no favorezcan la producción descontrolada de desechos, ni amplíen el problema de la contaminación de nuestras ciudades. Lamentablemente

la infraestructura obsoleta de nuestras ciudades ha venido colapsando y a diario se buscan establecer más y mejores alternativas para solucionar estos problemas.

Es allí donde nace el concepto de ciudades inteligentes (CI), debido a que desde la tecnología se busca proporcionar servicios y resolver los problemas de las urbes, facilitando la movilidad, mejorando los servicios sociales, la sostenibilidad y la seguridad con una escucha activa y constante de las necesidades de los ciudadanos. De esa manera nacen productos que en sus primeras versiones buscan ofrecer servicios básicos y recolectar información en tiempo real que apalancan la toma de decisiones efectiva, la creación de nuevas y mejores herramientas enfocadas en proveer bienestar y disminuir el uso de recursos que cada vez son más limitados.

Entre los sistemas más utilizados se encuentran aquellos que mediante la instalación de sensores en las calles detectan lugares libres de parqueo y dan al usuario la posibilidad de alquilarlos generando ingresos a las ciudades y ayudando a los ciudadanos a que se desplacen de manera más efectiva por la ciudad. También se cuenta con sistemas que dependiendo del flujo vehicular controlan los semáforos y regulan el tráfico además de emitir alertas para que los agentes de tránsito lleguen a sitios donde es necesaria su intervención. Otras herramientas conectan los sistemas de control de flota de la ciudad y sistemas de información permitiendo al ciudadano conocer en cuánto tiempo pasará el bus correspondiente a la ruta que le permite llegar a su destino por el paradero más cercano.

Existen tecnologías que examinan la calidad del aire y del agua o sus niveles mediante sensores instalados en las fuentes de los recursos naturales lo que permite tomar decisiones en función de la información que van recibiendo en tiempo real. Incluso, existen otros sistemas que buscan resolver problemáticas medioambientales, por ejemplo, los sensores que detectan los peatones

y dependiendo de ello disminuyen la luminosidad de las calles cuando no hay nadie, generando ahorros significativos y protegiendo la fauna local de la contaminación lumínica.

Todos estos sistemas hacen uso de tecnologías que apalancan la construcción de ciudades inteligentes, dentro de estas tecnologías se destacan: IOT, los sistemas ciberfísicos, Big Data, Data analytics, Data Mining, Cloud computing, Realidad aumentada o mixta, Impresión 3D, Blockchain, Inteligencia artificial (IA), Drones, etc. Todas estas tecnologías generan, transmiten, transforman, consumen y almacenan gran cantidad de información, además de requerir disponibilidad 7x24 debido a que las ciudades se vuelven dependientes de estos sistemas para la prestación de sus servicios más básicos.

Existen desafíos asociados a la implantación de este tipo de tecnologías, tales como la conectividad, la estandarización de los equipos, la necesidad de integración, interoperabilidad, eficiencia energética, la calidad, frecuencia y sincronización de los datos dada las múltiples fuentes y formatos de cada uno de los componentes de las soluciones implantadas, así como la privacidad de los ciudadanos e instituciones son retos que constantemente deben ser abordados en los diseños de las ciudades inteligentes. No menos importante es el incremento de la seguridad de los dispositivos que son objetos de ataques físicos y la seguridad de la información que constantemente se vuelve objeto de trasgresión.

En torno a la ciberseguridad se hace necesario realizar un análisis exhaustivo de los riesgos asociados a la ciberdelincuencia que se pueden materializar en las soluciones que se implanten a nivel ciudad, para ello es necesario conocer el entorno, las tecnologías utilizadas y el negocio en sí mismo, de tal manera que se identifiquen buenas prácticas enfocadas en definir un marco de trabajo para el gobierno y gestión de la ciberseguridad para las ciudades digitales. Dentro

de esta actividad debemos definir y evaluar los niveles de seguridad de la información que deben estar inmersos en estos sistemas, en función de la confidencialidad, la integridad y la disponibilidad de la información.

4. JUSTIFICACIÓN

Transformar ciudades tradicionales en ciudades inteligentes, es un esfuerzo cada vez más necesario e importante, el crecimiento de la población en las zonas urbanas viene aumentando de manera significativa, pero con la ayuda de la tecnología digital, internet de las cosas (IoT) y tecnologías disruptivas, esa transformación en más factible. Estas tecnologías permiten integrar datos captados por dispositivos, analizarlos y con base en esa información mejorar la operatividad y la toma de decisiones en busca de ser más eficientes en la prestación de servicios públicos, transporte, seguridad y sostenibilidad.

Las ciudades, además de ser un espacio estratégico de concentración de flujos económicos, también son centros que reúnen y generan una gran cantidad de información y dónde ocurren los mayores avances tecnológicos y de innovación de los países. Sin embargo, cada vez más las tecnologías que soportan la recolección, almacenamiento y análisis de datos en las ciudades inteligentes (CI), son susceptibles a las amenazas de ciberataques. Ejemplo de ello, fue lo ocurrido en Dallas en abril de 2017, cuando 156 alarmas que se usan para avisar a la población de tornados y fuertes tormentas, fueron hackeadas y sonaron por dos horas ocasionando caos y pánico en la ciudad (BBC News, 2017).Y recientemente, los Estados Unidos declararon estado de emergencia, después de un ciberataque y robo de 100 GB de información a la mayor red de oleoductos del país, lo cual subió el precio de los combustibles y suspendió el suministro de los mismos (BBC News Mundo, 2021).

Estos tipos de ciberataques se están convirtiendo en algo más frecuente, debido a que la tecnología usada en estas CI es insegura y está expuesta si no se cuentan con los sistemas integrales de seguridad adecuados. Aunque es verdad que existen investigaciones particulares

que tratan de resolver cuestiones de seguridad en IoT, IA, Big Data y otros temas emergentes, no se realizan integrando todo el panorama de una CI en la que se recopila, almacena y analiza constantemente información de los ciudadanos. Por lo tanto, es aconsejable tomar muy en serio la ciberseguridad de las CI, pues son objetivos atractivos para el cibercrimen y las consecuencias pueden ser graves si no se toman medidas oportunas.

Teniendo presente que cada nuevo servicio TIC puede ser objeto de ataques por diferentes motivos y en un creciente nivel de complejidad, la ciberseguridad debe estar implícita desde el momento mismo de la concepción de los proyectos que buscan implantar soluciones tecnológicas y no convertir la ciberseguridad en una característica que se adhiere luego de construido. Para ello se definirá un marco de gobierno y gestión de ciberseguridad para ciudades inteligentes enfocado en la integración de tecnologías emergentes que nos permitan detectar fraudes, garantizar la operación y disminuir los ataques de los que podamos ser víctimas, logrando fortalecer la confianza en las soluciones digitales por parte del estado y los ciudadanos.

De esta manera, el propósito de esta investigación es contribuir significativamente con la dirección, la gestión y el buen gobierno de la información de los ciudadanos de las ciudades de categoría I y II en Colombia, a través de marcos de referencia, donde se pueda optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y capital humano. Todo esto con el fin de integrar e institucionalizar las buenas prácticas, medir el valor y administrar el riesgo de las actividades inherentes de TI dentro de las CI, garantizando que TI apoye la seguridad de la información ciudadana.

5. OBJETIVO GENERAL

Diseñar un marco de gobierno y gestión de la ciberseguridad en el contexto de las ciudades inteligentes colombianas.

6. OBJETIVOS ESPECÍFICOS

1. Desarrollar una revisión sistemática de la literatura que permita obtener un panorama general sobre los estándares y normativas relacionadas con los marcos de ciberseguridad en el contexto de las ciudades inteligentes.

2. Elaborar un marco de gobierno y gestión de TI general, que incluya el componente de ciberseguridad para una ciudad inteligente.

3. Validar y probar el marco de gobierno y gestión de ciberseguridad propuesto para una ciudad intermedia en Colombia.

7. ALCANCE Y DELIMITACIÓN

El alcance de este proyecto, respecto al campo teórico que tocará, está suscrito a la seguridad de la información en Ciudades Inteligentes y al diseño de un marco de gobierno y gestión de ciberseguridad en las mismas soportadas en marcos de referencia aplicables a nivel ciudad.

En cuanto al alcance espacial del mismo, este serán ciudades colombianas de categoría I y II, alineada con las propuestas del Ministerio de las Telecomunicaciones de Colombia (MinTic).

8. METODOLOGÍA

La investigación estará desarrollada en varias fases, teniendo en cuenta que será bajo la perspectiva de investigación descriptiva que busca la definición, registro, análisis e interpretación de un fenómeno objeto de estudio. “La investigación descriptiva trabaja sobre realidades de hecho, y su característica fundamental es la de presentarnos una interpretación correcta” (Tamayo, 2003, P. 46).

Fase 1: Estudio e Investigación de Conceptos

En una primera fase se estudia y analiza el estado del arte del concepto, las teorías y modelos de ciberseguridad en ciudades inteligentes en el mundo; así como los acercamientos que se están haciendo en torno al tema de las vulnerabilidades y riesgos de seguridad de las ciudades inteligentes.

En una segunda parte se procede a analizar nuestra realidad colombiana, en torno al estado y avance nacional en la definición y aplicación de conceptos de ciberseguridad de ciudades inteligentes, así como aproximaciones locales para ciudades colombianas de categoría I y II.

- Fuentes primarias. Las fuentes de información primarias que se usarán son regulaciones y lineamientos de MinTic.
- Fuentes secundarias:

  a) Estándares y normas Internacionales relacionadas con la ciberseguridad de la información

  b) Artículos científicos de fuentes confiables relacionados con la seguridad de la información, ciudades inteligentes y ciberseguridad.

Fase 2: Diagnóstico de ciberseguridad en CI de Colombia.

En esta etapa, se determinará el estado actual y estado deseable en materia de ciberseguridad de las propuestas de CI en las ciudades en Colombia.

Para ello se realizará una matriz DOFA a modo de poder identificar las debilidades, oportunidades, fortalezas y amenazas existentes que pudieran afectar la ciberseguridad de la ciudad.

Fase 3: Diseño de marco de gobierno y gestión de la ciberseguridad propuesto

Luego de sintetizar las características del modelo que se quiere seguir según los estándares y marcos de referencia de ciberseguridad, se diseñará un marco de gobierno y gestión de la ciberseguridad en Ciudades Inteligentes para la realidad colombiana.

Fase 4: Validación del marco de gobierno y gestión diseñado

En esta etapa se pretende aplicar el marco de gobierno y gestión de ciberseguridad en el caso de estudio. Mediante indicadores se buscará hacer seguimiento y verificar la eficacia.

9. MARCO TEÓRICO

9.1 PROBLEMÁTICAS URBANAS

De acuerdo con el Departamento nacional de planeación los países con mayores tasas de urbanización tienen mayores niveles de ingresos, esto nos lleva a pensar que las tendencias de crecimiento y concentración de la población en las ciudades seguirá aumentando en el afán de lograr que nuestros países sean más competitivos y los ciudadanos tengamos mayor calidad de vida (DNP, 2018).

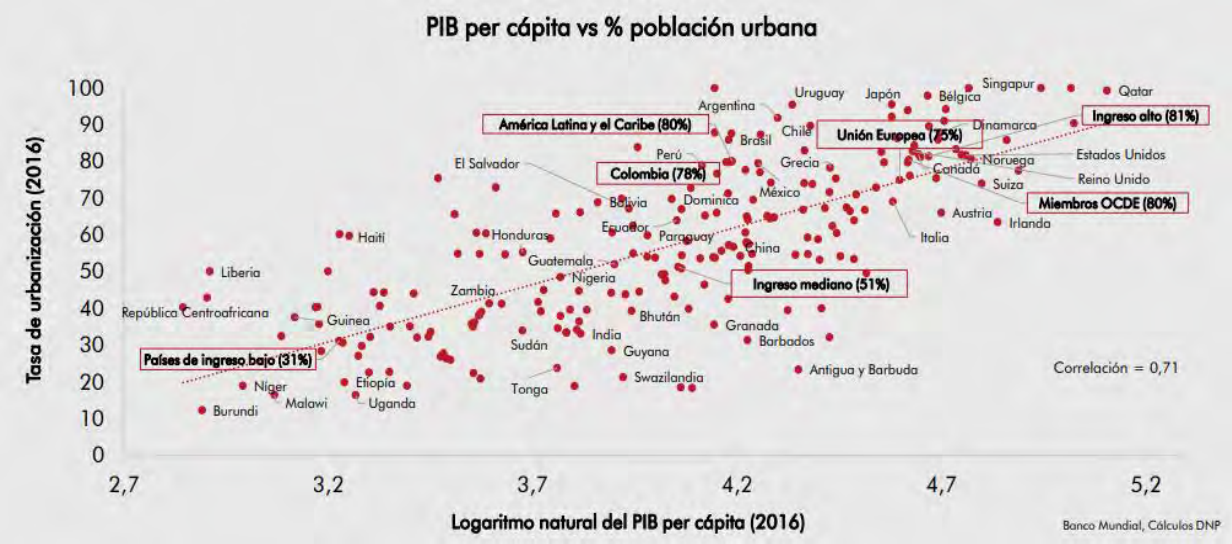

Figura # 1 Tasa de urbanización vs Población urbana

Para el caso de Colombia en las ciudades se observa que el índice de pobreza multidimensional es inversamente proporcional a la tasa de urbanización, encontrando que Chocó y La Guajira lideran el índice de pobreza, pero también tienen una población más pequeña a pesar de ser regiones ricas en recursos naturales que son ampliamente explotados a nivel nacional. Se estima que para el año 2050 en Colombia la población urbana aumentará en 14,5 millones y tendremos 69 ciudades con más de 100.000 habitantes.

Figura # 2 Población Urbana nacional
Fuente: UN-Habitat (2012) Misión sistema de ciudades para Colombia

Con el objetivo de aprovechar el incremento en las tasas de urbanización y convertirlo en algo positivo surgen retos en torno a:

- *Productividad*: Se busca la generación de ingresos a través de actividades no extractivas, en ese sentido Antioquia es la región de Colombia más productiva.
- *Conectividad*: Distancia media entre un municipio y el núcleo o ciudad uninodal por vía terrestre.
- *Seguridad*: Regularmente este reto está asociado a la tasa de homicidios (número de asesinatos por cada 100.000 habitantes), En este punto es importante considerar que Colombia tiene una tasa de 24.5 cifra mucho mayor que el promedio de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de 3.7. Las riñas y la delincuencia es un factor importante para considerar (OCDE, 2020).
- *Tecnología*: Para medir este índice se utiliza la velocidad promedio de ancho de banda, en Colombia solo 13 municipios registran velocidad de banda ancha (bajada) promedio superior a 25 Mbps a corte del 2019

- *Sostenibilidad*: una de las maneras de medirla es a través del índice de uso del agua[1], para el caso de Colombia el 66% de los municipios tienen presión alta o muy alta. Otra manera de medirlo es por la disposición de residuos sólidos.
- *Asociatividad:* esto corresponde a la prestación de servicios públicos y/o transporte. El 28% (308) de los municipios del país no tiene prestación de servicios regionales.
- *Equidad e Inclusión Social*: corresponde a cambios en la estructura de la población y oportunidades diferenciadas para su desarrollo.

Para superar estos retos es necesario abordar integralmente cada uno de ellos, mediante el uso de tecnologías de la información se busca proveer a las ciudades herramientas que propendan por el desarrollo y mejoramiento de cada uno de los frentes de trabajo necesarios para la modernización de las ciudades. Es allí donde nace el concepto de ciudades inteligentes.

9.2 CIUDADES INTELIGENTES

El Grupo Temático del ITU-T sobre ciudades inteligentes y sostenibles (FG-SSC) define una ciudad inteligente y sostenible como " *una ciudad innovadora que utiliza tecnologías de la información y la comunicación (TIC) y otros medios para mejorar la calidad de vida, la eficiencia de las operaciones y los servicios urbanos, y competitividad, garantizando al mismo tiempo que responda a las necesidades de las generaciones presentes y futuras en los aspectos económicos, sociales y medioambientales* ” (ITU, 2015).

Las ciudades inteligentes se caracterizan por un uso intensivo de la tecnología para el desarrollo y crecimiento de cada uno de los sistemas que las componen, desde sus servicios más básicos hasta los más complejos. Esto implica tener la capacidad de automatizar procesos que nos

[1] Índice de uso del agua: corresponde a la relación entre demanda y oferta hídrica superficial disponible y se clasifica así: > 50: Muy Alto, 20.01 a 50: Alto, 10.01 a 20: Moderado, 1 a 10: Bajo, Menor a 1: Muy Bajo

lleven a generar, recopilar, analizar, transformar y gestionar la información, de tal manera que sus procesos, productos y servicios sean cada vez de mejor calidad, lo que busca repercutir en la calidad de vida de los ciudadanos, la identificación y satisfacción de necesidades emergentes, la mejora de la productividad y competitividad, una toma de decisiones inteligentes apoyada en la información, y sostenibilidad ambiental.

Algunas de las soluciones que deben ser implementadas en las ciudades inteligentes se encuentran:

- Infraestructura: redes de sensores (IOT) para gestión de energía, agua y residuos.
- Energía: redes, medidores.
- Movilidad: gestión del tráfico, gestión del estacionamiento.
- Recaudo electrónico: sistemas que permiten hacer pagos a través de dispositivos sin contactos, códigos QR, Tarjetas inteligentes
- Conectividad: redes WiFi 4G gratuitas o superiores.
- Salud: sistemas de salud electrónica y Salud Móvil (m-Health).
- Seguridad cognitiva: seguridad para sistemas de información a través de una comprensión antropológica en conjunto con herramientas como la inteligencia artificial.
- Seguridad inteligente: seguridad para la infraestructura física.
- Educación: e-learning, tablero electrónico, proyector interactivo.
- Campus inteligente: todos los conceptos definidos para la ciudad inteligente aplicados a las universidades, que pueden considerarse para este concepto como una ciudad pequeña.

La seguridad es un factor crítico de éxito en este tipo de soluciones, dado que está en riesgo el normal desarrollo de servicios de los que dependemos todos los ciudadanos en menor o mayor medida y los ataques físicos a la infraestructura o cibernéticos son cada día más frecuentes, de acuerdo a un informe de tendencias del cibercrimen en Colombia a través de los canales de atención a empresas y ciudadanos dispuestos por la Policía Nacional fueron registrados 28.827 casos durante el 2019, un 58% más con respecto al 2018, pero esto no se detuvo allí, durante el 2020 debido a la pandemia y la cuarentena las cifras siguieron incrementando aún más los riesgos. Los ciberdelincuentes aprovecharon las vulnerabilidades propias del trabajo descentralizado y de los sistemas de información que terminaron más expuestos debido a la necesidad de garantizar prontamente la continuidad de las empresas, esto llevó a que los delincuentes encontraran grietas por donde filtrarse y las explotaron con diferentes tipos de ataques que van desde las estafas de phishing hasta el malware.

Ante este escenario al que se ven enfrentadas las ciudades, los retos de seguridad cibernética son inmensos, en gran parte debido a que la superficie de ataque de las ciudades inteligentes es muy extensa, lo que hace que resulte difícil reconocer y administrar cada una de las vulnerabilidades y sus respectivos impactos. Cualquier falla puede tener consecuencias desafortunadas tales como: Ausencia de los servicios públicos primordiales (Acueducto, energía, saneamiento básico, gas natural, alumbrado) o la ausencia del servicio de transporte público. Es por ello que las ciudades inteligentes necesitan estar diseñadas teniendo en cuenta la ciberseguridad, incorporándose desde su especificación, análisis, diseño y considerándola a lo largo de toda su vida útil. Se deben realizar de manera cíclica análisis y gestión de riesgos sobre distintas amenazas, test de penetración, simulaciones de ataques reales, etc.

9.3 SEGURIDAD Y CIBERSEGURIDAD

Antes de hablar de Ciberseguridad es necesario conocer el concepto básico de seguridad. La seguridad puede definirse como un estado en el cual los peligros y las condiciones que pueden provocar daños físico, psicológico o material son controlados para preservar la salud y el bienestar de los individuos y de la comunidad. De acuerdo al Programa de Naciones Unidas para el Desarrollo (PNUD) la definición de seguridad humana refiere a siete elementos (Mack A, 1994):

- Seguridad económica: los individuos deben tener garantizado un ingreso por encima de la línea de pobreza.
- Seguridad alimentaria: tener acceso a una correcta alimentación.
- Seguridad de la salud: protección frente a enfermedades infecciosas.
- Seguridad ambiental: protección del medio ambiente y sus recursos no renovables.
- Seguridad personal: cuidado frente a distintas formas de violencia e inseguridad.
- seguridad comunitaria: paz entre las distintas comunidades y la protección de sus identidades
- Seguridad política: protección de los derechos humanos

Una ciudad inteligente debe propender por garantizar estos elementos y para ello requiere tener una infraestructura que, de acuerdo con la Unión Internacional de Telecomunicaciones UIT, de la Organización de las Naciones Unidas tienen tres componentes: físico, de servicio y de las TIC o digital. La infraestructura física es lo que es verdaderamente "físico" o tangible - por ejemplo, edificios, vías de tren, carreteras, líneas eléctricas, tuberías de gas, de agua, fábricas y similares. Infraestructura de servicios es la superposición de servicios en los aspectos físicos - por ejemplo, un servicio de transporte, servicios públicos, la educación y el cuidado de la salud. La Infraestructura de las TIC es el núcleo y actúa como centro neurálgico, orquestando

todas las diferentes interacciones entre los diferentes elementos esenciales y la infraestructura física. (UIT, 2014)

La infraestructura de las TIC para una ciudad es muy compleja, debe estar hiperconectada y maneja volúmenes de datos exorbitantes, por lo que se pueden generar muchísimas vulnerabilidades que, con los procesos definidos, involucramiento de los interesados y buena gobernanza, se pueden proporcionar soluciones a los problemas relacionados con la ciberseguridad, la protección de la información y la resiliencia del sistema.

De acuerdo a ISACA la Ciberseguridad es la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

Por su parte la ITU en la resolución 181 define la ciberseguridad como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedia, y la totalidad de la información transmitida y/o almacenada en el ciberentorno (ITU, 2010).

Debido a que una amenaza a la ciberseguridad podría introducirse en la infraestructura de una ciudad inteligente y cualquiera que sea el lugar comprometido, el riesgo puede aumentar con rapidez ya que un sistema puede comprometer al siguiente, es necesario conocer los ataques

más frecuentes que sufren las ciudades, con el objetivo de tomar acciones preventivas y definir planes de acción en la medida que se materialicen estas vulnerabilidades:

- Man-in-the-middle: un atacante infringe, interrumpe o falsifica las comunicaciones entre dos sistemas.
- Datos y robo de identidad: la gran cantidad de información personal de los ciudadanos puede ser explotada por los ciberatacantes para transacciones fraudulentas o usurpar su identidad.
- Secuestro de dispositivos: El atacante secuestra y asume efectivamente el control de un dispositivo. Estos ataques pueden ser difíciles de detectar porque, en muchos casos, el atacante no altera la funcionalidad básica del dispositivo.
- Denegación de servicio distribuida (DDoS): intenta hacer que una máquina o recurso de red no esté disponible para sus usuarios previstos interrumpiendo temporal o indefinidamente los servicios de un host conectado a Internet.
- Denegación de servicio permanente (PDoS) o phlashing: ocasionan un daño en el dispositivo necesitando ser reemplazado o reinstalar su hardware.

Así, las ciudades inteligentes se convierten en entornos altamente heterogéneos y distribuidos, en los que implementar medidas de seguridad estándar es complejo y, en ocasiones, incluso inviable. Además, los datos de seguridad son difíciles de obtener en muchos casos porque las redes y los dispositivos normalmente son operados por proveedores externos.

9.4 INFRAESTRUCTURA TECNOLÓGICA DE UNA CIUDAD INTELIGENTE

Uno de los retos más complejos de afrontar en el momento que se busca alcanzar el concepto de una ciudad inteligente, es la definición de la infraestructura tecnológica que soportará dicha solución, que, dada su misma naturaleza heterogénea y de múltiples componentes, muchas veces interactuando entre sí de maneras no evidentes, hace que la escogencia de esta infraestructura, un paso importante.

Con el objetivo de que la implementación de una ciudad inteligente esté al alcance de cualquier ciudadano, se requiere que la infraestructura escogida sea basada en estándares abiertos, interoperable con cualquier tecnología compatible y agnóstica de marcas comerciales, con el fin de evitar una monopolización de fabricantes y su posterior decisión en el direccionamiento estratégico del plan de desarrollo de la ciudad.

Adicionalmente a esto, el fortalecimiento de las alianzas público-privadas, donde se logren la unificación de recursos financieros, tecnológicos y humanos, con el objetivo de alcanzar un objetivo común, es la piedra angular de los casos de éxito en ciudades pioneras en el concepto. En este sentido, lograr maximizar las ganancias de las empresas privadas, mientras se logra una disminución del gasto público en una ciudad, es una de las metas primordiales para alcanzar la integración de ambos actores, y lograr la transición a una ciudad innovadora.

Tomando por ejemplo la ciudad de Ámsterdam, donde se crearon institutos de investigación y desarrollo para iniciativas de soluciones urbanas (en áreas como acueducto, aseo, energía y gestión de los datos), donde tales institutos se encuentran abiertos a la colaboración de

instituciones educativas, empresas privadas, gobierno y residentes locales. (1) Estos institutos promueven la participación colaborativa de todos los actores de una ciudad, permitiendo la integración de soluciones en un nivel generalizado y no particular.

9.5 MARCOS DE REFERENCIA PARA LA GOBERNANZA DE LA CIBERSEGURIDAD

Los marcos de referencia buscan alinear la gestión de TI al negocio, asegurar el cumplimiento de objetivos, la creación de valor, gestionar los riesgos, administrar el uso adecuado de los recursos y mejorar el desempeño del gobierno de TI. Muchos de los marcos de referencia tienen gran aplicabilidad a nivel de empresas, pero no es sencillo llevarlos a nivel de ciudades, sin embargo, es posible a partir de ellos generar una serie de directrices que deben ser seguidas por cada uno de los sistemas críticos que componen las ciudades inteligentes. A continuación, se nombran algunos de los marcos de referencia que serán considerados en el diseño de marcos de gobierno y gestión de la ciberseguridad para ciudades inteligentes en el contexto colombiano.

NIST

En el año 2013 el entonces presidente de los Estados Unidos, Barack Obama emitió la orden Ejecutiva 13636 en la que se establece que es política de los Estados Unidos mejorar la seguridad y la resistencia de la infraestructura crítica de la nación y mantener un entorno cibernético que fomente la eficiencia, la innovación y la prosperidad económica al mismo tiempo que se promueve la seguridad, la confidencialidad empresarial, la privacidad y las libertades civiles. El Instituto nacional de estándares y tecnología (NIST) fue seleccionado para la tarea de desarrollar el marco porque es una agencia federal no reguladora que actúa como una fuente imparcial de datos y prácticas científicas, incluidas las prácticas de ciberseguridad. (NIST, 2018)

De esta forma nace este framework que, si bien puede ser aplicado en el entorno empresarial, tiene total aplicabilidad a nivel de ciudades inteligentes teniendo como objetivo reducir y gestionar de manera más eficiente los riesgos de seguridad cibernética. Este marco presenta

múltiples maneras de ser usado, a continuación, se mencionan las más relevantes que podrían ser implementadas a nivel ciudad:

- Revisión básica de prácticas de seguridad cibernética, mediante la comparación de las actividades actuales contra las definidas en el núcleo del framework, se definen las brechas y establece un plan de mejora que debe ser desarrollado por la ciudad a través de cada una de las secretarías u organismos de control encargados de los sistemas críticos y no críticos que se implementen.

- Establecimiento o mejora de un programa de seguridad cibernética, comenzando con el establecimiento de los objetivos y alcance de cada uno de los programas a implementar o implementados en una ciudad inteligente, pasando por la creación de un perfil actual, la realización de una evaluación de riesgos, la definición de una brecha e implementando un plan de acción.

- Comunicación de requisitos de seguridad cibernética a las partes interesadas, un sector de infraestructura crítica establece un perfil objetivo y se determina cuáles son los requisitos que hace falta implementar para llegar al objetivo planteado.

- Decisiones de compra, a partir de una lista de requisitos de seguridad cibernética el marco puede ser usado para tomar la mejor decisión de compra entre múltiples proveedores, comparando múltiples productos o servicios con brechas conocidas en el perfil objetivo. Una vez que se compra un producto o servicio, el perfil también se puede utilizar para identificar y abordar el riesgo de seguridad cibernética residual.

- Como metodología para proteger la privacidad y las libertades civiles, el gobierno y sus

agentes tienen la responsabilidad de proteger las libertades civiles derivadas de las actividades de seguridad cibernética. Para ello deben establecer un proceso que permita garantizar el cumplimiento de las actividades de seguridad cibernética con las leyes de privacidad, las reglamentaciones y los requisitos constitucionales aplicables a cada territorio.

ISO 37106

Ciudades y comunidades sostenibles: orientación sobre el establecimiento de modelos operativos de ciudades inteligentes para comunidades sostenibles. Es una guía que brinda orientación a los líderes en ciudades y comunidades inteligentes (de los sectores público, privado y voluntario) sobre cómo desarrollar un modelo operativo abierto, colaborativo, centrado en los ciudadanos y habilitado digitalmente para su ciudad que ponga su visión de un futuro sostenible en funcionamiento (ISO, 2018a).

Centrándose en:

- Hacer que las necesidades de los ciudadanos actuales y futuros sean la fuerza impulsora detrás de la toma de decisiones de inversión, la planificación y la entrega de todos los espacios y sistemas de la ciudad
- Integrar la planificación física y digital
- Identificar, anticipar y responder a los desafíos emergentes de manera sistemática, ágil y sostenible
- Crear un cambio radical en la capacidad para la entrega conjunta y la innovación a través de los límites organizacionales dentro de la ciudad.

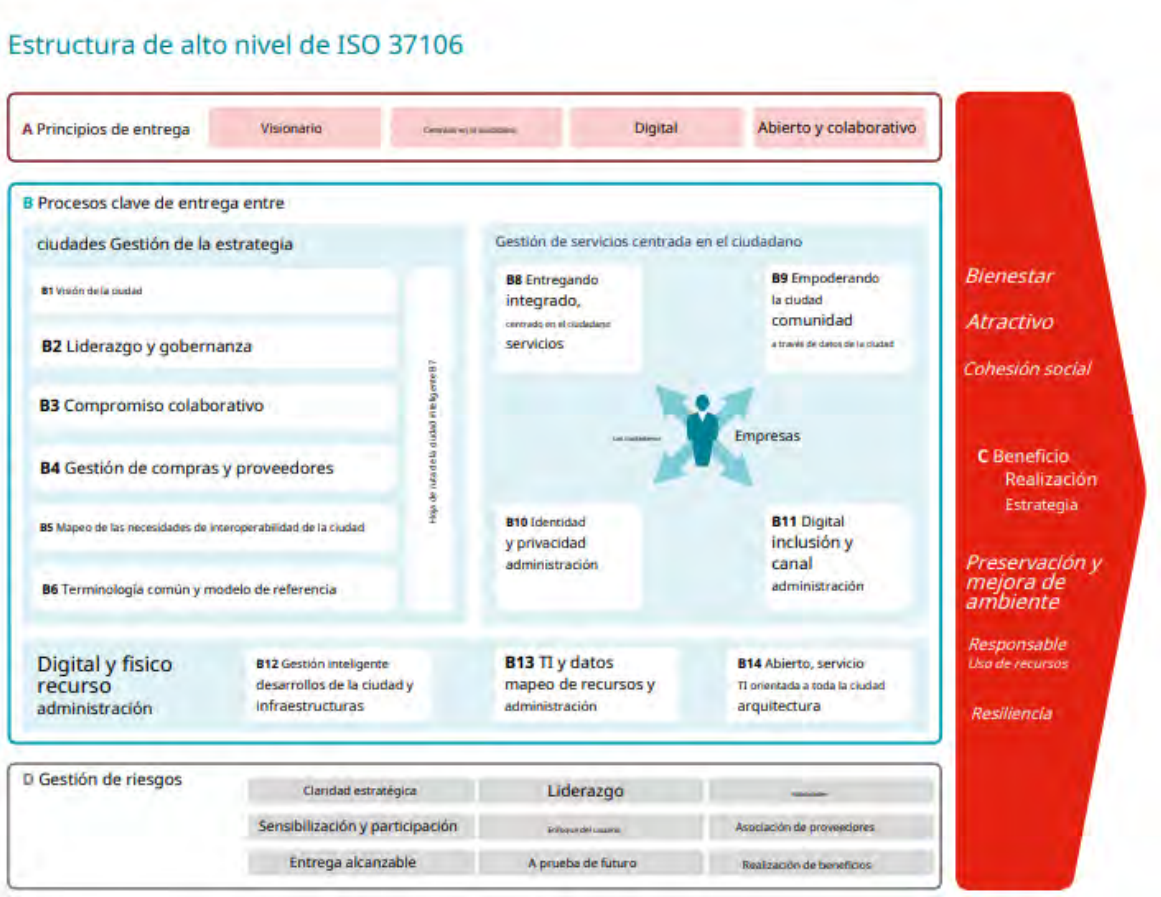

Figura # 3 Estructura de alto nivel de ISO 37106

Esta norma proporciona herramientas comprobadas que las ciudades pueden implementar al poner en práctica la visión, la estrategia y la agenda de políticas que se han desarrollado tras la adopción de ISO 37101, el sistema de gestión para el desarrollo sostenible de las comunidades. También puede ser utilizado, total o parcialmente, por ciudades que no se han comprometido a implementar el sistema de gestión ISO 37101.

ISO 37106 reúne las mejores prácticas comprobadas de ciudades de todo el mundo sobre cómo gestionar la transición de ciudades aisladas a ciudades inteligentes con éxito.

ISO 37120:2018

Desarrollo sostenible de comunidades. Indicadores para los servicios de las ciudades y la calidad de vida. Esta norma busca ayudar a las ciudades a guiar y medir la gestión del desempeño de los servicios urbanos, así como la calidad de vida de las diferentes ciudades. Para esto define y establece metodologías que incluyen un conjunto de indicadores que permiten dirigir y medir el desempeño de los servicios de la ciudad y la calidad de vida de sus habitantes. (ISO, 2018b)

Este estándar es aplicable, independientemente de su tamaño o ubicación, a cualquier gobierno, ciudad o municipio. Busca establecer una metodología y un conjunto de indicadores normalizados que puedan ser utilizados por cualquier ente sin que se deban considerar las características de la ciudad, indicando como deben ser interpretados los resultados obtenidos.

La norma, documenta o recoge cien indicadores categorizados en diecisiete temas sobre servicios municipales y calidad de vida: transporte, planificación urbana, alcantarillado y tratamiento de aguas residuales, suministro de agua potable, economía, educación, energía, medio ambiente, finanzas, respuesta ante fuego y emergencias, gobernanza, sanidad, ocio / espacios de recreo, seguridad ciudadana, vivienda, residuos urbanos sólidos, telecomunicaciones e innovación.

ISO 27001

Es la norma principal de requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) en donde se enumeran objetivos de control y controles que se sugieren implementar en el SGSI.

ISO 27002

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Es la sustituta de ISO17799:2005, y que contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

ISO 27005

Es una guía para la gestión del riesgo de la seguridad de la información.

Las normas técnicas y estándares ayudan a las ciudades inteligentes a alinear la oferta de soluciones tecnológicas con la ciberseguridad y tratamiento de riesgos de seguridad informática. Existen muchas normas dedicadas al modelo general de Ciudades Inteligentes pero que no tocan a profundidad la ciberseguridad. Por otro lado, hay normas de ciberseguridad que, aunque no fueron diseñadas para ciudades sino para organizaciones, se pueden usar para generalizar estrategias a nivel territorial considerando las ciudades como una empresa u organización compleja.

Las CI usan el IoT para alcanzar sus objetivos de sostenibilidad, energía, movilidad entre otras. En la literatura analizada, se encontraron muchos estudios y análisis de seguridad para IoT y esto sumado a los estándares internacionales supone una garantía de seguridad y privacidad a los usuarios. Por lo tanto, para la siguiente fase de este estudio, es necesario revisar y unificar esos estándares de IoT y aplicarlos a CI.

10. MODELO PROPUESTO

10.1DIMENSIONES DE UNA CIUDAD INTELIGENTE

Todos los territorios buscan lograr una sostenibilidad a nivel social, económico y medioambiental, para cumplir este objetivo se requiere trazar un plan estratégico de la ciudad e implementar estrategias de incorporación organizada de la tecnología, de tal manera que se logren acoplar los distintos componentes que hacen para de las plataformas del ecosistema digital.

Para lograr construir el plan estratégico de una ciudad inteligente se hace necesario hacer un diagnóstico previo de la ciudad en materia de innovación y transformación digital para cada una de las dimensiones que hacen parte de una ciudad inteligente, para el contexto colombiano se evaluarán 6 dimensiones que nos deben llevar a dar pasos en la dirección correcta. El gráfico siguiente muestra dichas dimensiones.

Figura # 4 Dimensiones de una ciudad inteligente

Para el análisis de las dimensiones tomaremos como referencia el modelo de Estonia (e-estonia), un país báltico que ha sido reconocido con el título de primera nación digital del mundo. Un lugar donde el 99% de las interacciones con el Estado pueden realizarse online. Este país logró recuperar su independencia en 1991 y con un pequeño presupuesto, pero con un gran talento informático decidió apostarle a digitalización debido a que no podía ofrecer estructuras burocráticas tradicionales (E-Estonia,2021).

Dimensión 1: Datos

Para que un territorio pueda avanzar en la oferta de servicios digitales es necesario que cuente con una plataforma de interoperabilidad que conecte todas las instituciones, de tal manera que, las diferentes organizaciones estatales y algunas privadas pueden intercambiar información en un mismo formato para poder prestar los servicios que requieren los ciudadanos. En este sentido se debe considerar que la plataforma sea distribuida, modular, segura, garantizando la confidencialidad, integridad e interoperabilidad entre las partes que intercambian datos.

Figura # 5 Dimensión 1 – Datos

Fuente: Elaboración propia

E-identity es otro de los pilares de una ciudad inteligente, se trata de un mecanismo a través del cual los ciudadanos pueden demostrar su identidad en línea, lo que habilita una serie de trámites y servicios rápidos, seguros y sin la necesidad de desplazarse. Para implementar identificación digital se pueden utilizar tarjetas con chips que contienen archivos con información de registro civil de nacimiento, historia clínica, licencia de conducción y cualquier

otra información que resulte útil para el ecosistema digital, para el caso de Estonia el 99% de las personas cuenta con estas tarjetas.

Otra opción es usar el teléfono móvil como una forma de identificación digital segura, para ello se utiliza e instala una SIM que además ser utilizada como la tarjeta de identificación y permitir acceder a los servicios digitales, permite firmar documentos digitalmente que son legalmente vinculantes, con la ventaja de no requerir un lector de tarjetas, lo cual disminuye los costos de implementación y la hace inclusiva dado que no se requiere un teléfono inteligente.

Para las personas que cuentan con un teléfono inteligente o tablet pueden utilizar APPs que solo necesitan una conexión a la red móvil o wifi. Para el año 2018 Estonia implementó Smart-ID, una APP que se ha reconocido como QSCD (dispositivo cualificado de creación de firma). Este es el nivel más alto de reconocimiento en la UE, y en la actualidad todos los usuarios de Smart-ID pueden firmar digitalmente documentos en el nivel de firma electrónica cualificada (QES) que deben ser reconocidos por cada Estado miembro de la Unión Europea.

Finalmente, la seguridad es esencial para mantener la fiabilidad de los datos, evitar la pérdida, acceso no permitido, integridad y la disponibilidad de la información. Para dar respuesta a este pilar en las bases de datos del gobierno de Estonia se implementó la tecnología Blockchain, lo que garantiza la autenticidad de los datos electrónicos matemáticamente. Esto significa que nadie, ni los administradores del sistema, ni el gobierno de turno, puede manipular los datos.

Dimensión 5: Gobierno digital

En un territorio que busca una transformación hacia una ciudad inteligente es indispensable que el estado avance hacia la implementación de las tecnologías de la información disruptivas que le permitan ofrecerle al ciudadano servicios en línea, automatizados y centrados en el usuario.

Figura # 6 Dimensión 2 – Gobierno digital
Fuente: Elaboración propia

En este sentido cobra vital importancia el tema de la dimensión de datos descrita anteriormente, en donde el ciudadano está plenamente identificado y se tiene su información más relevante consolidada, lo que permitirá ofrecer servicios en línea por defecto eliminando trámites burocráticos innecesarios, reduciendo costos y tiempos de atención. Un ejemplo de ello son las votaciones en línea que ya se tiene implementadas en varios países.

Al tener los diferentes sistemas interconectados una ciudad contará con suficiente información para una toma de decisiones eficiente, basada en:

- Identificación de los objetivos y fuentes de datos clave.
- Exploración de la data.
- Detección y comprensión de tendencias, valores atípicos y los patrones de comportamiento.
- Análisis de los resultados y toma de medidas a partir de la información.
- Por último, es de vital importancia que esta información se socialice con los actores que tienen alguna interacción con los datos examinados y deben tomar decisiones en este sentido.

Para el gobierno estonio está dimensión tiene un enfoque aún mayor, una vez tuvieron mucho de sus servicios en línea pensaron en ¿por qué no hacer que la administración se ponga en contacto con los ciudadanos para ofrecer los servicios cuando se tenga conocimiento que ciudadano tiene derecho a ellos? Lo anterior con el objetivo de disminuir aún más la carga de la burocracia, tanto para las personas como para el estado.

Una de las preocupaciones más grande de esta dimensión es la privacidad y el temor a las filtraciones de seguridad, que algunas veces han superado el valor percibido del intercambio de información. Sin embargo, un habilitador clave de las ciudades inteligentes sostenibles es el hecho de que todos los participantes del ecosistema complejo comparten información y la combinan con datos contextuales que se analizan en tiempo real.

Dimensión 3: Educación

La educación es una de las dimensiones más importantes en cualquier sociedad, para el caso puntual de las ciudades digitales se busca que la tecnología sea un habilitador de los procesos de enseñanza, para ello se imparte formación TIC desde muy temprana edad con el objetivo de garantizar que el estudiante adquiera los conocimientos y destrezas necesarias para acceder a la infraestructura digital para su uso actual y futuro.

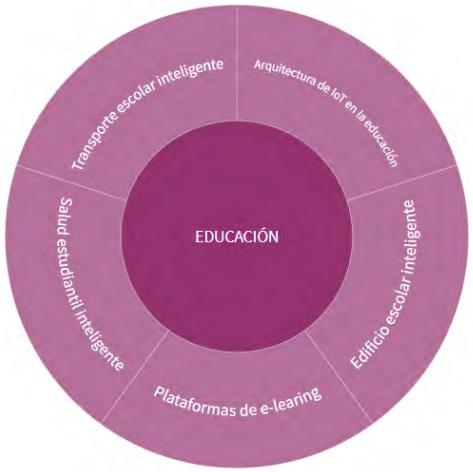

Figura # 7 Dimensión 3 - Educación

Fuente: Elaboración propia

Con la pandemia causada por el virus Covid-19 se puso en evidencia las dificultades que tienen muchas nacionales en materia del e-learning, la falta de cobertura de las redes, recursos digitales y de dispositivos de conexión para cada estudiante, puso en jaque a muchas instituciones educativas de todos los niveles. Es necesario aclarar que los sistemas de e-learing no deben ser meros contenedores de contenido digital, la información debe ser transmitida de acuerdo con los modelos y patrones pedagógicamente definidos para afrontar los retos de estos nuevos contextos. Tecnológicamente el proceso de enseñanza se sustenta en aplicaciones de software de entornos web, desplegados en infraestructura elástica que permitirá ajustarse de acuerdo con los periodos académicos.

El e-learning permite reducir el ausentismo de las clases, acceder a materiales educativos a costos más bajos, a través de firmas digitales asegurar que los niños no puedan faltar a la escuela o intentar falsificar una nota de sus padres, ahorrar tiempo de los profesores y estudiantes y verificar las calificaciones en línea por los acudientes.

Estonia ha desplegado estrategias de aprendizaje permanente, porque entiende que las expectativas del sector privado en relación con el capital humano están en pleno cambio. Por lo tanto, tanto las empresas estatales como las privadas ofrecen una variedad de cursos de TI (a menudo gratuitos) para los interesados de cualquier edad. De esta forma, se ofrece a las personas la oportunidad de formarse e incrementar sus habilidades de TI, al tiempo que facilita la realización de los cambios necesarios en sus elecciones profesionales.

Adicionalmente dentro del tema educativo se debe avanzar en la implementación de tecnología IOT que permita tener la cobertura de donde están los niños y adolescentes desde el momento que toman las rutas estudiantiles, dentro de las instalaciones del centro educativo, hasta tener

el control en cuanto a la integridad física del estudiante, para ello se podrá saber si el estudiante es remitido a enfermería, tener acceso a su historia clínica para su revisión y brindar una mejor atención, poder registrar una evento tipo accidente, alergia o cualquier otra novedad.

Con la implementación de IOT, RFID, WSN y la nube se pueden recopilar datos relacionados con la eficiencia del alumno y métodos de aprendizaje aplicados; Asimismo, los educadores pueden utilizar para mejorar el desempeño de todos los objetos educativos (Estudiantes, Educadores y otras herramientas). IoT está impactando la vida cotidiana. Puede proponer muchas ventajas en varios segmentos relacionados con los esquemas de aprendizaje. (Bayani M., Leiton K. & Loaiza M.,2017)

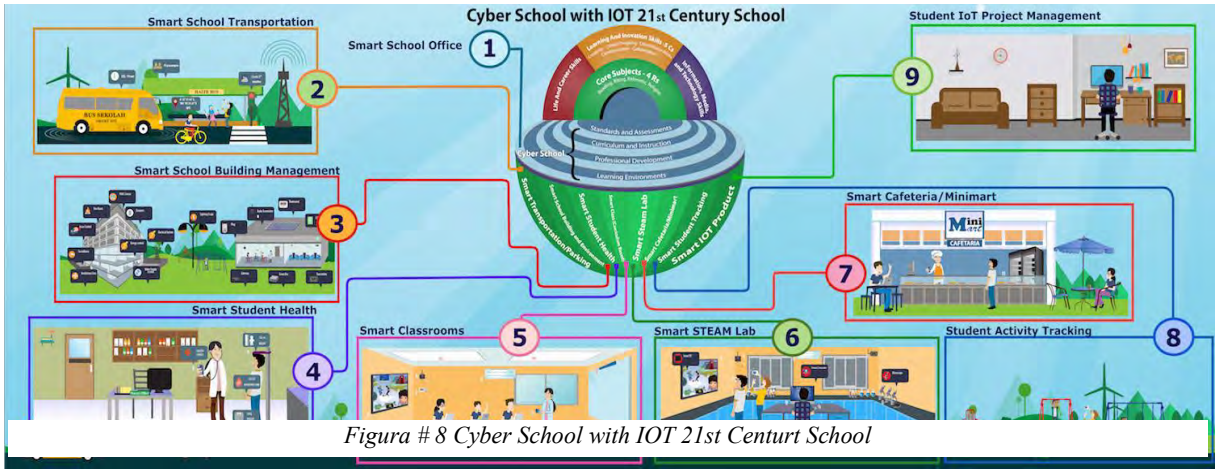

Figura # 8 Cyber School with IOT 21st Centurt School

Fuente: http://www.cyberschool.id/content/iot-education

Dimensión 4: Movilidad

La movilidad inteligente es una de las dimensiones con más desarrollo en el entorno de las ciudades digitales, comenzando con el uso de tarjetas NFC para el recaudo electrónico de los sistemas de transporte público, pasando por implementaciones de sistemas de inteligencia artificial para definir frecuencias de despacho considerando las variables de tiempo, horario, época del año, ruta, etc y finalizando con sistemas de Internet de las cosas (IoT) que permiten hacer una gestión más apropiada de los recursos con el objetivo de lograr transiciones a sistemas de transporte "Verdes", seguros y sostenibles.

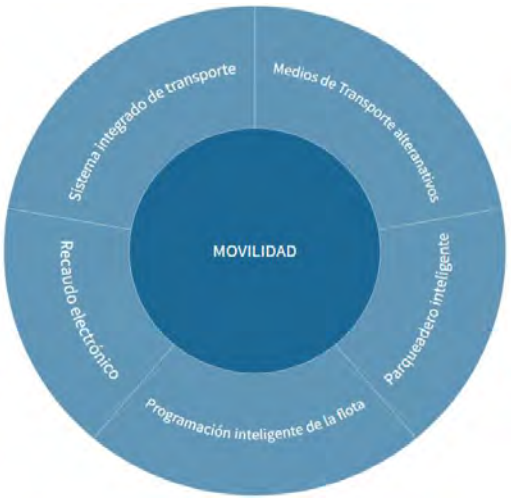

Figura # 9 Dimensión 4 - Movilidad
Fuente: Elaboración propia

Son muchos los dispositivos de IoT interconectados para satisfacer las necesidades de los sistemas de transporte inteligentes, estos dispositivos producen un enorme volumen de datos. Sin embargo, la protección de la privacidad se ha convertido en uno de los mayores problemas con el progreso de los macrodatos. La privacidad personal generalmente se ve desafiada por el desarrollo de la tecnología. La preferencia móvil de las personas puede explotarse para realizar ataques de reidentificación. La privacidad, seguridad de los canales de comunicación, la autenticación, autorización del usuario y privacidad de los datos que contiene información profundamente sensible son variables para considerar dado que pueden causar graves daños a la privacidad de la identidad de los ciudadanos si se tienen en cuenta los datos de trayectoria generados en sistemas de transporte inteligentes. (Behrendt, 2016)

Dimensión 5: Servicios públicos

Los servicios públicos tales como la Energía, Alumbrado público, Acueducto, Alcantarillado, Aseo, Gas natural, Internet, Telefonía pueden parecer estáticos en el desarrollo de ciudades inteligentes, sin embargo, son de los sectores que mayor apropiación de nuevas tecnologías han realizado en los últimos años, esto debido a la imperiosa necesidad de ofrecer servicios que sean sostenibles en el tiempo dado la creciente población mundial minimizando el impacto ambiental. En este sentido Colombia dentro de los objetivos de desarrollo sostenible para el año 2030 presenta alguno de las siguientes metas. DNP (MARZO 2018):

Figura # 10 Dimensión 5 – Servicios públicos

Fuente: Elaboración propia

- Acceso universal a servicios energéticos asequibles, fiables y modernos
- Invertir y Facilitar el Acceso a Investigación y Tecnología en Energía Limpia, incluidas las fuentes renovables, la eficiencia energética y las tecnologías avanzadas y menos contaminantes
- Aumentar el porcentaje global de energía renovable
- Agua potable segura y asequible: lograr el acceso universal y equitativo al agua potable a un precio asequible para todos
- Mejorar la calidad del agua, el tratamiento de aguas residuales y la reutilización segura
- Gestión integrada de los recursos hídricos y cooperación transfronteriza
- Proteger y Restaurar los Ecosistemas Hídricos de agua dulce
- Acceso universal a tecnologías de la información y las comunicaciones.

Para cumplir con estas metas Colombia ha venido trabajando en la incorporación de tecnologías de la cuarta revolución industrial, tales como sensores de IOT, medidores inteligentes, luminarias sensibles al movimiento, y se esperan implementaciones en realidad aumentada para mejorar la ejecución de los trabajos de campo, reducir tiempos y costos operativos.

Dimensión 6: Salud

«La salud es un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades». La cita procede del Preámbulo de la Constitución de la Organización Mundial de la Salud, que fue adoptada por la Conferencia Sanitaria Internacional, celebrada en Nueva York del 19 de junio al 22 de julio de 1946, firmada el 22 de julio de 1946 por los representantes de 61 Estados (Official Records of the World Health Organization, Nº 2, p. 100), y entró en vigor el 7 de abril de 1948. La definición no ha sido modificada desde 1948.

Figura # 11 Dimensión 6 – Salud
Fuente: Elaboración propia

Dentro del contexto de ciudades inteligentes son muchas las implicaciones que tiene la salud no solo a nivel individual sino a nivel de salud pública, mucho más después de la pandemia por el virus SARS-CoV-2 de la gran familia de los coronavirus. Es necesario garantizar la cobertura, excelente prestación de servicios, planes de prevención y control de enfermedades, así como planes de creación y deporte que garanticen el bienestar de los ciudadanos. La tecnología es un gran habilitador dentro de todos estos planes comenzando con el manejo de la información de cada individuo, su historia clínica digital, el uso de mecanismos de diagnóstico, imágenes diagnosticas, telemedicina, el uso de los teléfonos inteligentes y los dispositivos

como pulseras, relojes u otros accesorios permiten la monitorización de las condiciones de salud de las personas y posteriormente la toma de decisiones por parte de los profesionales de la salud.

10.2 CONTROLES DE SEGURIDAD PARA UNA CIUDAD INTELIGENTE

Luego de revisar los distintos estándares se propone tomar como principal referencia el estándar de seguridad NIST, seleccionar los principales controles que tienen aplicabilidad al contexto de ciberseguridad para una ciudad inteligente y complementarlo con algunos controles de ISO 27001 e ISO 37106. A continuación, se listas los controles seleccionados:

FUNCIÓN	CATEGORÍA	SUBCATEGORÍA
IDENTIFICAR	Gestión de activos (ID.AM)	Las plataformas de software y las aplicaciones dentro del ecosistema de la ciudad están inventariadas.
		Los sistemas de información externos están catalogados.
		Los dispositivos de IOT u otros que prestan servicios están inventariados
	Entorno empresarial (ID.BE)	Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen y acuerdan tanto para sistemas propios como externos para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).
	Gobernanza (ID. GV)	Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.
		Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.
		Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.
	Evaluación de riesgos (ID.RA)	Se identifican y se documentan las amenazas, tanto internas como externas.
		Se identifican y priorizan las respuestas al riesgo.
	Estrategia de gestión de riesgos (ID.RM)	Los actores de la organización y externos establecen, gestionan y acuerdan los procesos de gestión de riesgos.

	Gestión del riesgo de la cadena de suministro (ID.SC)	Los actores y los socios externos identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.
		Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.
PROTEGER (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC)	Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.
		Se autentican los usuarios, dispositivos y otros activos acordes al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).
	Seguridad de los datos (PR.DS)	Se mantiene una capacidad adecuada para asegurar la disponibilidad.
		Se implementan protecciones contra las filtraciones de datos.
		Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.
	Procesos y procedimientos de protección de la información (PR.IP)	Se realizan, se mantienen y se prueban copias de seguridad de la información.
		Definir cómo medir la efectividad de los controles o grupos de controles seleccionados
		Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).
	Tecnología de protección (PR.PT)	Las redes de comunicaciones y control están protegidas.
		Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente) para lograr los requisitos de resiliencia en situaciones normales y adversas.
DETECTAR (DE)	Anomalías y Eventos (DE.AE)	Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.
		Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.
		Se determina el impacto de los eventos.
	Monitoreo Continuo de la Seguridad (DE.CM)	Se monitorea la red para detectar posibles eventos de seguridad cibernética.
		Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.
		Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.
	Procesos de Detección (DE.DP)	Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
		Los procesos de detección se mejoran continuamente.

RESPONDER (RS)	Planificación de la Respuesta (RS.RP)	El plan de respuesta se ejecuta durante o después de un incidente.
	Comunicaciones (RS.CO)	Los incidentes se informan de acuerdo con los criterios establecidos.
		La información se comparte de acuerdo con los planes de respuesta.
		La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.
	Análisis (RS.AN)	Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).
	Mitigación (RS.MI)	Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.
	Mejoras (RS.IM)	Los planes de respuesta incorporan las lecciones aprendidas.
		Se implementan las mejoras identificadas y se e actualizan las estrategias de respuesta.
RECUPERAR (RC)	Planificación de la recuperación (RC.RP)	El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.
	Mejoras (RC.IM)	Se actualizan las estrategias de recuperación.
	Comunicaciones (RC.CO)	Se gestionan las relaciones públicas.
		La reputación se repara después de un incidente.
		Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.

Tabla 1. Controles a implementar

10.3 NIVELES DE MADUREZ

Los modelos de Madurez pueden definirse como una herramienta que permite medir los diferentes aspectos de un proceso u organización, teniendo en cuenta que cada uno de estos aspectos deben tener una evolución en el tiempo para llegar al estado de madurez, donde la organización evaluada logra el máximo nivel de desempeño. Los modelos de madurez suelen tener niveles cada uno con un nombre, una descripción, un grupo de procesos, una serie de actividades con el detalle de cómo puede desarrollar las habilidades de cada nivel para dicha actividad.

Todo lo que puede ser medido tiene la posibilidad de ser mejorado y justamente ese es el propósito de un modelo de madurez, proveer una referencia para el mejoramiento de los procesos, evaluando sus fortalezas y debilidades, estableciendo comparaciones con otros organismos similares. De esta manera se permite establecer el nivel de madurez en que se encuentra el proceso, las posibilidades de mejora y por tanto establecer una hoja de ruta que lleve a una organización, ciudad y en general a cualquier organismo a un proceso de mejora continua en cualquier aspecto que sea evaluado

Para el desarrollo del presente documento se tomará como referencia los niveles de madurez definidos en el Modelo Integrado de Madurez de Capacidades CMMI V2.0, que consiste en un conjunto de buenas prácticas que brindan la posibilidad de mejorar el rendimiento de los procesos fundamentales de una organización. Este modelo fue desarrollado por miembros pertenecientes a la industria y el instituto de CMMI. A continuación, se muestran los niveles definidos en el modelo y las características que tiene cada uno.

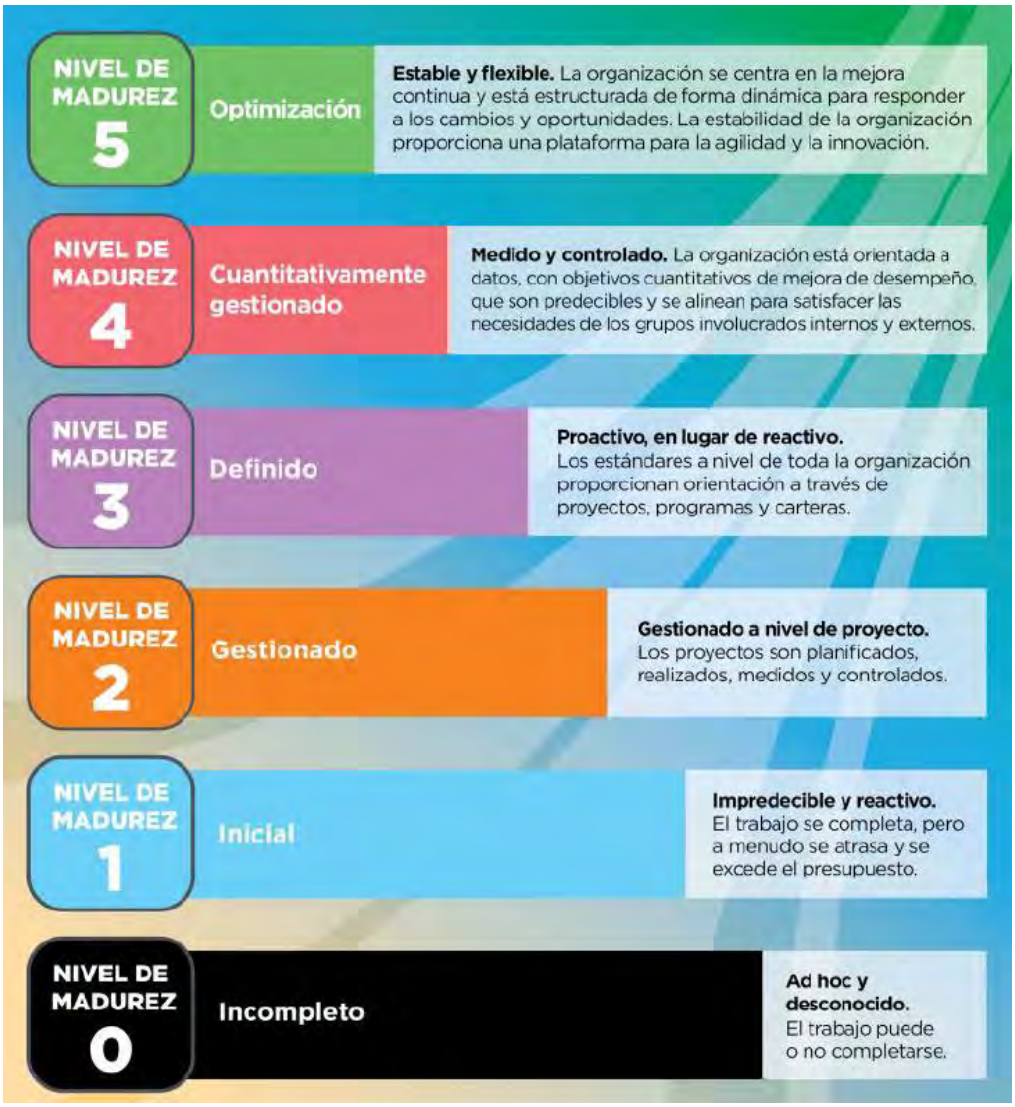

Figura # 12 Niveles de Madurez CMMI

Estos niveles nos llevaran desde una ciudad en su estado inicial sin políticas ni proyectos para convertirse en una ciudad inteligente, pasando por un ciudad reactiva, posteriormente llegar a ser un territorio gestionado, proactivo y optimizado en donde la tecnología está inmersa en la mayoría de los aspectos de la vida de los ciudadanos. A partir del listado de controles que se definieron previamente, se listan por cada subcategoría seleccionada el nivel de madurez al que pertenece, teniendo en cuanta las características de cada nivel definido por el modelo CMMI

Categoría	Subcategoría	Nivel del control
Gestión de activos (ID.AM)	Las plataformas de software y las aplicaciones dentro del ecosistema de la ciudad están inventariadas.	2
	Los sistemas de información externos están catalogados.	2
	Los dispositivos de IOT u otros que prestan servicios están inventariados	2
Entorno empresarial (ID.BE)	Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen y acuerdan tanto para sistemas propios como externos para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	4
Gobernanza (ID. GV)	Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	1
	Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	4
	Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	3
Evaluación de riesgos (ID.RA)	Se identifican y se documentan las amenazas, tanto internas como externas.	2
	Se identifican y priorizan las respuestas al riesgo.	1
Estrategia de gestión de riesgos (ID.RM)	Los actores de la organización y externos establecen, gestionan y acuerdan los procesos de gestión de riesgos.	3
Gestión del riesgo de la cadena de suministro (ID.SC)	Los actores y los socios externos identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	4
	Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	5
Gestión de identidad, autenticación y control de acceso (PR.AC)	Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	2
	Se autentican los usuarios, dispositivos y otros activos acordes al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	1
Seguridad de los datos (PR.DS)	Se mantiene una capacidad adecuada para asegurar la disponibilidad.	2
	Se implementan protecciones contra las filtraciones de datos.	2
	Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	4
Procesos y procedimientos de protección de la información (PR.IP)	Se realizan, se mantienen y se prueban copias de seguridad de la información.	2
	Definir cómo medir la efectividad de los controles o grupos de controles seleccionados	4
	Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de	4

	recuperación (Recuperación de Incidentes y Recuperación de Desastres).	
Tecnología de protección (PR.PT)	Las redes de comunicaciones y control están protegidas.	1
	Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente) para lograr los requisitos de resiliencia en situaciones normales y adversas.	4
Anomalías y Eventos (DE.AE)	Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.	2
	Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	4
	Se determina el impacto de los eventos.	1
Monitoreo Continuo de la Seguridad (DE.CM)	Se monitorea la red para detectar posibles eventos de seguridad cibernética.	1
	Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	3
	Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	2
Procesos de Detección (DE.DP)	Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.	4
	Los procesos de detección se mejoran continuamente.	5
Planificación de la Respuesta (RS.RP)	El plan de respuesta se ejecuta durante o después de un incidente.	1
Comunicaciones (RS.CO)	Los incidentes se informan de acuerdo con los criterios establecidos.	2
	La información se comparte de acuerdo con los planes de respuesta.	2
	La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	3
Análisis (RS.AN)	Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	3
Mitigación (RS.MI)	Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	2
Mejoras (RS.IM)	Los planes de respuesta incorporan las lecciones aprendidas.	4
	Se implementan las mejoras identificadas y se e actualizan las estrategias de respuesta.	5
Planificación de la recuperación (RC.RP)	El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	1
Mejoras (RC.IM)	Se actualizan las estrategias de recuperación.	5
Comunicaciones (RC.CO)	Se gestionan las relaciones públicas.	3
	La reputación se repara después de un incidente.	3
	Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	2

Tabla 2. Clasificación de controles por niveles de madurez

10.4 ROLES Y RESPOSABILIDADES

Una vez se definen los controles aplicables a nivel de una ciudad el siguiente paso es definir quienes serán los encargados del cumplimiento de cada uno de los controles, para ello se tomaron los roles establecidos en COBIT y se complementaron con los característicos en una ciudad, distrito o municipio, generando una matriz RACI en la que se puede asignar y definir el grado de responsabilidad que le corresponde a cada una de las personas que están involucradas en la realización de un proyecto o proceso.

A nivel de una ciudad es importante tener en cuenta que un rol puede ser ejecutado por una o varias personas, dependiendo de la naturaleza del servicio algunas aplicaciones pueden depender directamente del organismo público y muchas otras están en manos de privados a través de concesiones en donde se encuentra un operador del servicio y un facilitador tecnológico que soporta las soluciones necesarias para que los ciudadanos puedan disfrutar del servicio ofrecido, A continuación se listas cada uno de los roles con su respectiva descripción:

Rol	**Descripción**
Alcalde	Individuo que se encuentra al frente de la administración pública de una ciudad, distrito o municipio.
Ejecutivo de Negocio - secretario de alguna dependencia	Individuo responsable de la operación de una unidad de negocio específica, para el caso de una ciudad se tomará la unidad de negocio como una secretaría, por tanto, este rol corresponde a un secretario de alguna dependencia, por ejemplo: secretario general de educación.
Cumplimiento	Responsable de dirigir el cumplimiento legal, regulatorio y contractual, para este caso correspondería al secretario jurídico.

Gerente de Servicios	Individuo que gestiona el desarrollo, implementación, evaluación y gestión continua de nuevos y existentes productos y servicios para los ciudadanos.
Gerente de Seguridad de la Información	Individuo que gestiona, diseña, supervisa y/o evalúa la seguridad de la información de las diferentes plataformas que prestan servicios a nivel de la ciudad.
Gerente de Continuidad del Negocio	Individuo que gestiona, diseña, supervisa y/o evalúa las capacidades de la continuidad del servicio, para garantizar que las funciones críticas de la ciudad continúan operando ante eventos disruptivos.
Oficial de Privacidad	Individuo responsable de la supervisión de los riesgos e impactos para el servicio de las leyes de privacidad, de la dirección, coordinación e implementación de políticas y actividades que garanticen que se alcanzan las directivas de privacidad que esperan los ciudadanos.
Director General de Riesgos (CRO)	El ejecutivo de mayor cargo responsable de todos los aspectos de la gestión de riesgos para la ciudad. Se puede establecer un directivo de riesgos de TI para supervisar los riesgos relacionados con TI.
Director de Informática/Sistemas (CIO)	El ejecutivo de mayor cargo responsable de alinear TI con las estrategias de la política pública, también es responsable de que se planifique, se consigan los recursos necesarios y se gestione la entrega de servicios y soluciones de TI para soportar los objetivos de la ciudad.
Auditoría	Dependencia responsable de proveer auditorías, que garanticen el correcto cumplimiento de los procesos establecidos. A nivel

	de una ciudad también se podría considerar como una interventoría si el servicio es prestado por un ente privado
Comité de Estrategia de TI	Un grupo de ejecutivos de alto cargo designado por el Consejo para asegurar que el Consejo está involucrado y se mantiene informado de las cuestiones y decisiones más relevantes de TI. El comité es responsable de que se haga la gestión de la cartera de inversiones facilitadas por TI, los servicios de TI y los activos de TI, asegurando que el valor es entregado y el riesgo gestionado. El comité es normalmente presidido por un miembro del Consejo y no por el CIO
Oficina de Gestión de Programas y Proyectos (PMO)	La función responsable de apoyar a los gerentes de programas y proyectos, recopilando, evaluando y notificando información sobre la conducción de sus programas y proyectos que los constituyen
Jefe de Operaciones de TI	Individuos responsables de los entornos y la infraestructura para las operaciones de TI.
Operador del servicio	Empresa encargada de proveer el servicio que se brinda a nivel de la ciudad, por ejemplo: empresa encargada del sistema integrado de transporte.
Proveedor Tecnológico del servicio	Empresa encargada de proveer la tecnología que soporta el servicio que se brinda a nivel de la ciudad

Tabla 3. Roles

Luego de listar los roles más relevantes y los diferentes controles que buscan garantizar que una ciudad cuente con entornos ciberseguros se plantea una matriz RACI que permite tener claro las responsabilidades de cada actor frente a las distintas actividades que se deben ejecutar para tener gobierno y gestión de la ciberseguridad en cualquier ciudad.

Función	Categoría	Subcategoría	Alcalde	Secretario de dependencia	Secretario jurídico	Gerente de Servicios	Gerente de Seguridad de la Información	Gerente de Continuidad del Negocio	Oficial de Privacidad	Director General de Riesgos (CRO)	Director de Informática (CIO)	Auditoría	Comité de Estrategia de TI	PMO	Jefe de Operaciones de TI	Operador del servicio	Proveedor Tecnológico del servicio
Identificar	Gestión de activos (ID.AM)	Las plataformas de software y las aplicaciones dentro del ecosistema de la ciudad están inventariadas.				I	I	I	I		A		I	I	R		
		Los sistemas de información externos están catalogados.				I	I	I	I		A		I	I	R		
		Los dispositivos de IOT u otros que prestan servicios están inventariados				I	I	I	I		A		I	I	R		
	Entorno empresarial (ID.BE)	Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen y acuerdan tanto para sistemas propios como externos para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).				I	C	R	C	C	A		C	C	R	R	R
	Gobernanza (ID. GV)	Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.				I	R	C	C		A		R	I	R	I	R
		Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.			A	C	R	R	R	C	I	I	I	I	I	I	I
		Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.				I	C	C	C	R	A	I	C	C	C	I	I
	Evaluación de riesgos (ID.RA)	Se identifican y se documentan las amenazas, tanto internas como externas.					R	R	C	R	A	I	I	C	R	I	C
		Se identifican y priorizan las respuestas al riesgo.					R	R	C	R	A	I	C	C	R	I	C

	Estrategia de gestión de riesgos (ID.RM)	Los actores de la organización y externos establecen, gestionan y acuerdan los procesos de gestión de riesgos.				C	C	C	C	R	R	I	A	I	R	R	R
	Gestión del riesgo de la cadena de suministro (ID.SC)	Los actores y los socios externos identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.				C	C	C	C	A	R	I	C	I	I	R	R
		Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.			I	C	I	I	I	C	A	R	C	I	C	R	R
Proteger (PR)	Gestión de identidad, autenticación y control de acceso (PR.AC)	Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.				I	I	I	A	C	I		I	R	R	I	R
		Se autentican los usuarios, dispositivos y otros activos acordes al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).				I	I	I	A	C	I		I	R	R	I	R
	Seguridad de los datos (PR.DS)	Se mantiene una capacidad adecuada para asegurar la disponibilidad.				I	C	C	I	I	A		C	C	R	I	R
		Se implementan protecciones contra las filtraciones de datos.				I	C	C	R	I	A		C	C	R	I	R
		Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.					C	I	C	I	A	R	C	I	I	I	C
	Procesos y procedimientos de protección de la información (PR.IP)	Se realizan, se mantienen y se prueban copias de seguridad de la información.					R	R	I	I	A				I		R
		Definir cómo medir la efectividad de los controles o grupos de controles seleccionados				I	I	I	I	I	R		A	I	I	I	R

		Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).				I	R	R	I	C	A	I	C	I	R	I	R
	Tecnología de protección (PR.PT)	Las redes de comunicaciones y control están protegidas.								I	A				R		R
		Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente) para lograr los requisitos de resiliencia en situaciones normales y adversas.								I	A				R		R
Detectar (DE)	Anomalías y Eventos (DE.AE)	Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.					R	I	I	C	A		C		C	I	R
		Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.				I	R	C	I	C	A		C		C	I	R
		Se determina el impacto de los eventos.				I	R	C	I	C	A		C		C	I	R
	Monitoreo Continuo de la Seguridad (DE.CM)	Se monitorea la red para detectar posibles eventos de seguridad cibernética.				I	R	I	I	C	A		C		C	I	R
		Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.				I	R	C	I	C	A		C		C	I	R
		Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.				I	R	C	I	C	A		C		C	I	R
	Procesos de Detección (DE.DP)	Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.				I	R	I	I	C	R	A	C		C	I	R
		Los procesos de detección se mejoran continuamente.				I	R	I	I	C	A	I	C		C	I	R
Responder (RS)	Planificación de la Respuesta (RS.RP)	El plan de respuesta se ejecuta durante o después de un incidente.				I	R	R	I	C	A		C	I	C	I	R

	Comunicaciones (RS.CO)	Los incidentes se informan de acuerdo con los criterios establecidos.				I	R	R	I	C	A		C	I	C	I	R
		La información se comparte de acuerdo con los planes de respuesta.				I	R	R	I	C	A		C	I	C	I	R
		La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.				I	R	R	I	C	A		C	I	C	I	R
	Análisis (RS.AN)	Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).				I	C	C	I	R	A		C	I	C	I	R
	Mitigación (RS.MI)	Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.				I	C	C	I	R	A		C	I	R	I	R
	Mejoras (RS.IM)	Los planes de respuesta incorporan las lecciones aprendidas.				I	R	R	I	R	A		C	I	C	I	R
		Se implementan las mejoras identificadas y se actualizan las estrategias de respuesta.				I	R	R	I	C	A		C	I	C	I	R
Recuperar (RC)	Planificación de la recuperación (RC.RP)	El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.				I	C	R	C	C	A		I	I	C	I	R
	Mejoras (RC.IM)	Se actualizan las estrategias de recuperación.				I	C	R	C	C	A		R	I	C	I	R
	Comunicaciones (RC.CO)	Se gestionan las relaciones públicas.	I	A		C	C	C	C	C	R		C			C	C
		La reputación se repara después de un incidente.	I	A		C	C	C	C	C	R		C			C	C
		Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.		I	I	I	I	R	I	I	A		C		C	I	C

Tabla 4. Matriz RACI

10.5 MARCO PROPUESTO PARA EL GOBIERNO Y GESTIÓN DE LA CIBERSEGURIDAD DE LAS CIUDADES INTELIGENTES

Luego de revisar las dimensiones necesarias para el desarrollo de una ciudad inteligente en el contexto colombiano, los estándares de seguridad y ciberseguridad de la industria, seleccionar controles necesarios, definir los niveles de madurez, roles y responsabilidades se hace necesario establecer el marco integrado de gobierno y gestión de la ciberseguridad en donde se establezca la articulación entre la capa estratégica de la ciudad y la capa estratégica de TI así como su relación con las dimensiones previamente definidas, los estándares seleccionados, los procesos, proyectos requeridos y la estructura organizativa que se debe implementar desde lo publico sin olvidar que mucho de este trabajo se desarrolla de la mano de privados quienes a través de licitaciones públicas participan en el desarrollo, implementación y monitoreo de plataformas tecnológicas que soportan los servicios que se les prestan a los ciudadanos.

Teniendo en cuenta todos estos requerimientos, lineamientos, programas, proyectos, políticas y regulaciones se estableció un marco de gobierno y gestión de la ciberseguridad para ciudades inteligentes en el contexto colombiano, para empezar, se definieron dos (2) grandes grupos de requerimientos que alimentan el modelo, el primero de ellos está asociados a las siguientes aristas:

- Tecnologías disruptivas tales como Big data, IOT, Inteligencia artificial, Realidad aumentada o mixta, Blockchain, Inteligencia artificial (IA), Gemelo digital, Drones, Computación en la nube, Redes móviles 5G, etc que vienen a dar solución a muchas problemáticas pero que su implementación trae consigo otros retos tecnológicos tales como la conectividad, estandarización de los equipos, integración de las distintas plataformas, interoperabilidad y la ciberseguridad. Toda esta tecnología mal usada

puede afectar los objetivos de la ciudad, la institucionalidad y la calidad de vida de las personas.

- La regulación vigente a nivel de seguridad de la información (para el caso colombiano está definida en la Tabla #6. Marco regulatorio para la ciberseguridad en Colombia del presente documento).
- La privacidad de los ciudadanos y el manejo de los datos personales.
- Los requerimientos del estado y las mismas alcaldías que requieren desarrollar e impulsar programas que propendan por el bienestar de los ciudadanos.
- La disponibilidad, confidencialidad e integridad de la información, que para el caso de una ciudad es un factor crítico de éxito
- La gestión estratégica de riesgos de tecnología informática, que involucra tanto la gestión de la continuidad como la administración de riesgos.

Por otro lado, el segundo grupo de requerimiento está representado por las dimensiones definidas para la ciudad inteligente: Datos, Salud, Movilidad, Servicios públicos, Educación y gobierno digital. Cada una de estas dimensiones traen consigo necesidades que deben ser analizadas y resueltas con el apoyo de la tecnología, mediante de un portafolio de proyectos que buscan cerrar la brecha entre el estado actual y el estado objetivo.

A continuación, se ilustra el modelo propuesto, que cuenta con cinco capas, que nos llevan desde donde queremos estar, resolviendo las inquietudes ¿Dónde estamos ahora? y ¿cómo llegamos a donde queremos estar?, para finalmente dar respuesta a revisar ¿cómo lo estamos haciendo? y como lo mejoramos.

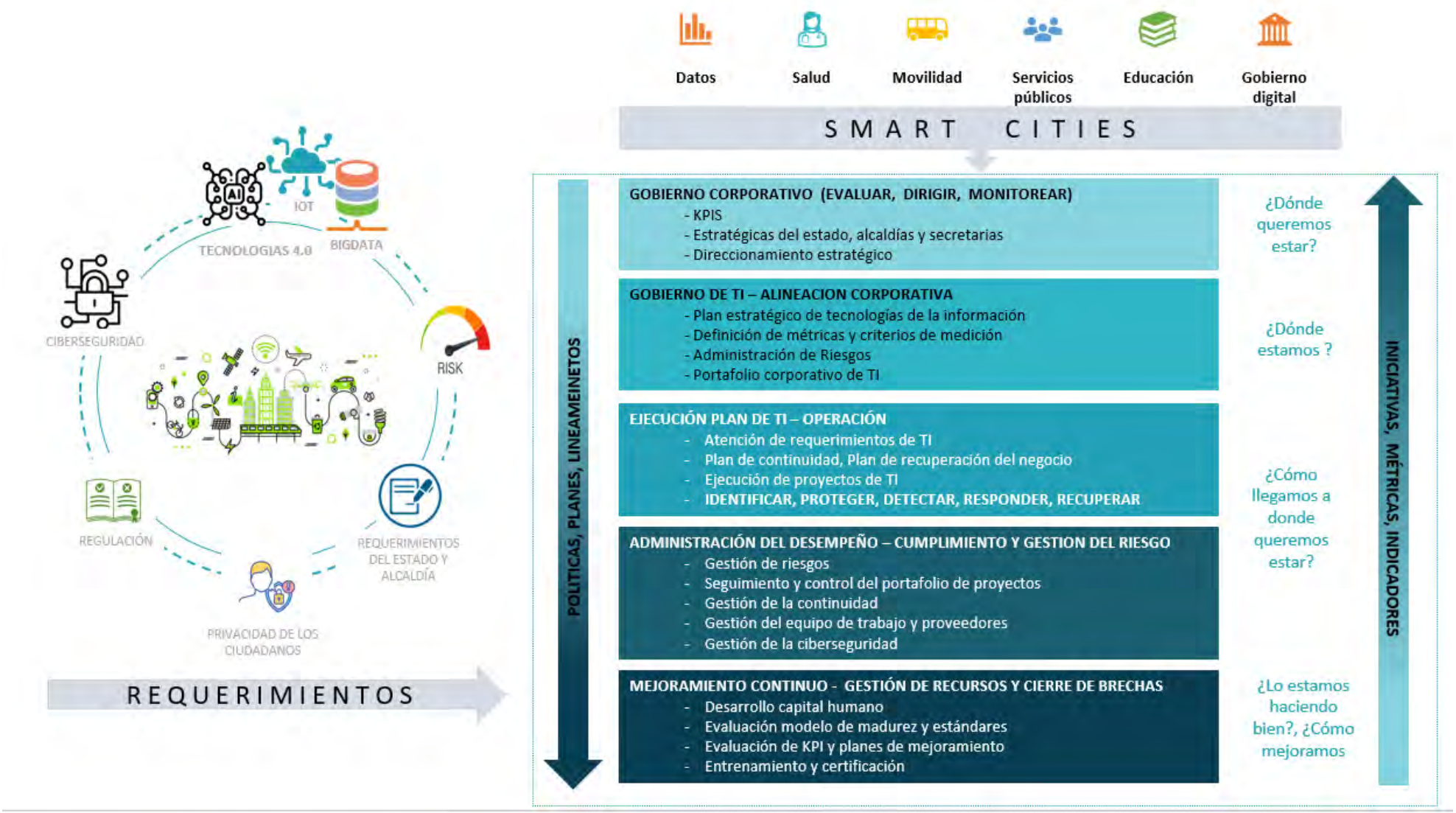

Figura # 13 Modelo propuesto

10.5.1 GOBIERNO CORPORATIVO

Para comenzar se debe definir una primera capa de "Gobierno corporativo", que en este contexto es un Gobierno de ciudad que define y vela por la implementación y cumplimiento de políticas públicas que garanticen que la ciudad se va a desarrollar de la manera que los ciudadanos esperan, en este sentido desde el gobierno nacional se ha venido trabajado en una serie de políticas en torno de cada una de las dimensiones antes mencionadas a través de cada uno de los correspondientes ministerios.

Particularmente desde el Ministerio de Tecnologías de la Información y las Comunicaciones, que según la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones en nuestro país, se vienen trabajando una serie de estrategias, iniciativas y políticas en pro del desarrollo de los territorios y del bienestar de los ciudadanos, una de sus principales funciones del ministerio es aumentar y facilitar el acceso de todos los ciudadanos del territorio nacional a las tecnologías de la información, de tal manera que se promueva la inversión y se cierre la brecha digital para contribuir al desarrollo económico y social de la nación, mejorando el bienestar de los colombianos. A continuación, se listan algunas de las políticas, iniciativas y proyectos que hacen parte de la capa estratégica que se ha definido a través del ministerio:

Políticas, iniciativas y/o proyectos	Breve descripción
Gobierno digital	Política de Gobierno nacional que define los lineamientos, estándares y proyectos estratégicos, que permiten llevar a cabo la transformación digital del Estado, a fin de lograr una mejor interacción con los ciudadanos, usuarios y grupos de interés; De esta manera se busca dar

	respuesta a las necesidades de los ciudadanos y del estado, resolver problemáticas públicas, posibilitar el desarrollo sostenible y en general, crear valor público.
Misión TIC 2022	Programa con un gran objetivo: formar 100.000 jóvenes y adultos colombianos en programación, para enfrentar los desafíos de la Cuarta Revolución Industrial.
Datos abiertos	Iniciativa que tiene por objetivo promover y habilitar las condiciones para la apertura, uso y generación de valor a partir de datos abiertos de gobierno. Estos datos son publicados en el portal de datos abiertos del estado colombiano
Arquitectura TI de Colombia	Práctica estratégica con un enfoque metodológico que deben adoptar las organizaciones estatales con el fin de establecer una ruta para su transformación digital. Aplica para el desarrollo de nuevas soluciones tecnológicas, la automatización de proceso, tramites o servicios, proyectos de transformación digital y proyectos del PETI.
Centros de Transformación Digital Empresarial	Estrategia que tiene como objetivo acompañar a las mipyme en su proceso de transformación digital mediante la apropiación de tecnologías como una estrategia, que les ayudará a mejorar su productividad y competitividad.
Ciudades y territorios inteligentes	Iniciativa del Ministerio TIC que impulsa el desarrollo de ciudades y territorios inteligentes en todas las regiones de Colombia por medio de la implementación de la Política de Gobierno Digital. Se sustenta en una estrategia de fortalecimiento de capacidades mediante el acompañamiento especializado, asesoría consultiva, así como la apropiación del Modelo de Medición de Madurez de Ciudades y Territorios Inteligentes. Todas estas herramientas permiten la definición de una hoja de ruta para que las entidades territoriales puedan avanzar en su transformación digital territorial.
ConVerTIC	Proyecto de inclusión del Ministerio TIC con el fin de promover la inclusión social, educativa, laboral y cultural a través de uso de las tecnologías para las personas ciegas o con baja visión.
Centro de Relevo	Iniciativa del ministerio y la Federación Nacional de Sordos que apoyándose en la tecnología permite la comunicación en doble vía entre personas sordas y oyentes a través de una plataforma tecnológica que cuenta con intérpretes de la lengua de señas colombiana (LSC) en línea, teniendo a su disposición un intérprete del Centro de Relevo. Adicionalmente ofrece contenidos y espacios donde la lengua de señas y la lengua escrita prevalecen, el aprendizaje, la comprensión, construcción de conocimientos y sobre todo la motivación al uso de las TIC en las personas sordas, siendo no sólo consumidores sino productores de información.
EnTicConfio+	Programa de MinTic que promueve el desarrollo de las habilidades digitales para enfrentar con seguridad los riesgos asociados al uso de

	internet y las TIC. Así mismo, impulsa el uso y la apropiación de internet como la oportunidad para generar una huella digital positiva en el entorno digital. Este programa permite desarrollar habilidades para la identificación de riesgos, la promoción de la convivencia y el activismo digital, así como la utilización de herramientas tecnológicas para la movilización de causas solidarias y positivas en Internet.
Máxima Velocidad	Estrategia de aprendizaje que traslada el potencial de juegos al ámbito educativo que busca fortalecer las capacidades de TI de las entidades públicas mediante el desarrollo de retos enfocados a cada uno de los elementos que conforman la política de Gobierno Digital.
Centros digitales	Proyecto que busca prestar el servicio de Internet a sedes educativas rurales oficiales, comunidades indígenas, parques naturales, guarniciones militares y puestos de salud.

Tabla 5. Estrategias, iniciativas y programas del ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC, 2022).

Teniendo en cuenta que uno de los temas más importantes en el desarrollo de una ciudad inteligente es la ciberseguridad, debido a los millones de datos los que se manejan y la seguridad de la información es fundamental, para ello desde la capa estratégica de Gobierno se deben definir políticas que propendan por garantizar la integridad, confidencialidad y disponibilidad de la información que se maneja en las ciudades, estas políticas se ven reflejadas en el siguiente marco normativo:

Normatividad	Año	Descripción
Políticas técnicas de seguridad de la información Función Pública	2020	La declaración de la Política de Seguridad de la Información institucional busca proteger los activos de información (grupos de valor, información, procesos, tecnologías de información incluido el hardware y el software), mediante el establecimiento de lineamientos generales para la aplicación de la seguridad de la información en la gestión de los procesos internos, bajo el marco del Modelo Integrado de Planeación y Gestión, consolidada en los procedimientos, guías, instructivos y publicaciones, así como la asignación de roles y responsabilidades
Decreto 103 de 2015	2019	Compendio de políticas aplican para todos los servidores públicos y contratistas de Función Pública que procesan y/o manejan información de la entidad.

Decreto 1494 de 2015	2019	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley 1712 de 2014	2018	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.
Decreto 2573 de 2014	2018	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 1377 de 2013	2018	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 2609 de 2012.	2017	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley estatutaria 1581 de 2012	2017	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	2017	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Decreto 4632 de 2011	2017	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1273 de 2009	2016	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 527 de 1999	2015	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Constitución Política de Colombia1991 - Artículo 15	2015	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
Ley 23 de 1982	2015	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre y el Estado debe respetarlos y hacerlos respetar.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Ley 1581 de 2012	2012	Por la cual se dictan disposiciones generales para la protección de datos personales

Tabla 6. Marco regulatorio para la ciberseguridad en Colombia (MINTIC, 2022).

Para el cumplimiento del marco regulatorio el estado colombiano debe establecer una hoja de ruta de la estrategia de ciberseguridad alineada con los objetivos, metas, procesos, procedimientos y estructura organizacional de cada uno de los territorios que van avanzando hacia el desarrollo de una ciudad inteligente.

Esta capa del modelo está liderada por el alcalde de la ciudad acompañado del Comité directivo o consejo municipal según se conozca en el territorio y un Comité ejecutivo que en este caso en particular está confirmada por el grupo de secretarios designados por el alcalde, este órgano se encarga del direccionamiento estratégico, regular el cumplimiento de normas, atraer la inversión, mejorar la calidad financiera, asegurar la gestión de riesgos y la ciberseguridad, así como el logro de metas y el crecimiento de la ciudad. Adicionalmente cuenta con el Balance Scored Card(BSC) corporativo, que es una herramienta con la que se busca definir y garantizar el cumplimiento de las estrategias de forma dinámica e integral, mediante una serie de indicadores que evalúan el desempeño de los proyectos y las iniciativas.

10.5.2 GOBIERNO DE TI

Esta capa del modelo es la encargada de la alineación de TI con el gobierno corporativo de tal manera que se garantice el cumplimiento de los objetivos que se trazó la alta dirección en cabeza del alcalde de la ciudad, para ello constantemente se está evaluando y monitoreando las necesidades, requerimientos, proyectos de la ciudad con el objetivo de definir planes, procesos y proyectos de TI que acompañados con la asignación de recursos financieros y humanos, la adquisición o desarrollo de herramientas y la implementación de buenas prácticas y estándares

tales como ITIL, COBIT, ISO 27000, NIST, SCRUM, PMBOK de buscan satisfacer los objetivos planteados.

Con relación a la ciberseguridad se busca definir marcos de referencia aplicables que ayuden a alinear y priorizar las actividades de seguridad cibernética con las necesidades y requisitos de la ciudad, la tolerancia al riesgo y los recursos disponibles. Regularmente se utilizan niveles de implementación como un mecanismo para que las organizaciones comprendan su enfoque para gestionar el riesgo de seguridad cibernética, lo que ayudará a priorizar mejoras y alcanzar los objetivos de la seguridad.

De acuerdo con los roles previamente definidos el Gobierno y gestión de IT está representado en la estructura organizacional por el Director de Informática/Sistemas (CIO), Comité de Estrategia de TI, el Gerente de Seguridad de la Información y el Gerente de Continuidad del Negocio. Adicionalmente se podría considerar a MINTIC en cabeza del ministro y los viceministros de transformación digital y de conectividad como un aliado estratégico de esta capa, dado que a nivel nacional es el encargado de realizar esta labor y por consiguiente de definir políticas, lineamientos y planes que se convierten en un requerimiento para cada ciudad.

A nivel general en esta capa se define:

- El plan estratégico de tecnologías de la información
- Las métricas y criterios de medición de cada uno de los procesos de TI ejecutados.
- La administración de riesgos de Ciberseguridad y gestión de continuidad de los servicios, esto nos brinda la capacidad de cuantificar y comunicar los ajustes a sus programas de seguridad cibernética. Cada ciudad puede darle un manejo diferente a los riesgos, incluida la mitigación, la transferencia, la evasión o la aceptación del riesgo, dependiendo del impacto potencial en la prestación de los servicios críticos.

- El portafolio de proyectos de TI
- La arquitectura empresarial de la ciudad
- Gestión de tecnologías disruptivas
- La Infraestructura tecnológica que se debe desplegarse teniendo en cuenta la conectividad de los dispositivos en terreno, las necesidades de integración de cada una de las plataformas desplegadas, la interoperabilidad de los sistemas, la calidad, frecuencia y sincronización de los datos, preservando la privacidad de los ciudadanos e instituciones.

10.5.3 EJECUCIÓN DE PLANES DE TI

La siguiente capa del modelo es una capa de ejecución de los planes, proyectos y estrategias definidos con en la capa de gobierno de TI y de mantener en operación cada uno de los servicios que se prestan a nivel de la ciudad, De acuerdo con los roles previamente definidos de esta capa hacen parte: Gerente de Servicios, Gerente de Seguridad de la Información, Gerente de Continuidad del Negocio, Oficial de Privacidad, Oficina de Gestión de Programas y Proyectos (PMO), Jefe de Operaciones de TI, así como entes privados representados por el Operador del servicio y los proveedores Tecnológicos.

Los procesos que regularmente se ejecutan en esta capa son:

- Atención de requerimientos de TI procedentes de cada una de las secretarias, ministerios y dependencias que hacen parte de la ciudad.
- Ejecución de proyectos de TI previamente aprobados por el gobierno de TI.
- Instanciación del plan de continuidad del servicio, esto es, se desarrollan cada una de las actividades necesarias para que los servicios priorizados estén disponibles aun cuando se presente alguna situación que afecte la normal ejecución de estos, ya sea por un desastre natural, un ataque cibernético, falla de infraestructura o humana, etc.

- Gestión de la ciberseguridad: se ejecuta mediante los controles de seguridad para una ciudad inteligente definidos en el presente documento, cuyas principales funciones son: IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER, RECUPERAR, cada una de estas funciones ayudan a expresar la gestión del riesgo de seguridad cibernética a nivel macro, organizando información, abordando amenazas y mejorando el aprendizaje de actividades previas. Adicionalmente se complementa con la gestión de incidentes y ayuda a mostrar el impacto de las inversiones en ciberseguridad.

10.5.4 ADMINISTRACIÓN DEL DESEMPEÑO

Esta capa está definida con el objetivo de evaluar el desempeño del TI, realizando seguimiento a cada una de las actividades que se ejecutan por disposición del gobierno de tecnologías de la información y comunicaciones, son muchas las tareas a evaluar, pero dentro de las más representativas encontramos:

- Seguimiento y control del portafolio de los proyectos.
- Gestión de la continuidad del servicio.
- Gestión del equipo de trabajo y proveedores.
- Gestión de la ciberseguridad.
- Gestión de la infraestructura.
- Seguimiento y control al tratamiento de riesgos

De acuerdo con los roles previamente definidos, los procesos que hacen parte de esta capa son ejecutados por: el Director de Informática/Sistemas (CIO), Director General de Riesgos (CRO), Gerente de Seguridad de la Información, Gerente de Continuidad del Negocio, Oficial de Privacidad, Jefe de Operaciones de TI.

10.5.5 MEJORAMIENTO CONTINUO

La última capa del modelo es la de mejoramiento continuo, para ello es ideal utilizar los niveles de madurez definidos en el presente documento, en los que se busca evaluar la implementación y desempeño de cada uno de los controles definidos para la gestión de la ciberseguridad al interior de la ciudad. Para ello se propone seguir los siguientes pasos:

- Identificar y describir el estado actual de seguridad cibernética en que se encuentra la ciudad en materia de infraestructura, datos, procesos y proyectos.
- Describir los objetivos esperados de la ciberseguridad.
- Identificar y priorizar oportunidades de mejora de manera continua.
- Evaluar el progreso hacia los objetivos planteados.
- Comunicar entre las partes interesadas internas y externas sobre el riesgo de seguridad cibernética existente, controles implementados, el manejo otorgado a cada amenaza, los planes de mejora en curso y la brecha aun existente con los objetivos.

Estas actividades se deben ejecutar de manera periódica y deben ir acompañadas del desarrollo de las habilidades y competencias del capital humano de TI, socialización de estrategias implementadas, evaluación y mejoramiento del modelo de madurez propuesto, revisión de estándares aplicables, revisión y evaluación de KPIs definidos por el gobierno de TI, y planes de mejoramiento de herramientas, productos y servicios utilizados para la gestión de la ciberseguridad, así como entrenamiento y certificación de las personas e instituciones.

11. CASO DE ESTUDIO

A continuación, se aborda la validación del marco de gobierno y gestión de la ciberseguridad para ciudades inteligentes para el caso de estudio seleccionado: Ciudades colombianas de categoría I y II, antes de empezar es importante resaltar que el ministerio de Tecnologías de la Información y las Comunicaciones de Colombia ha estado trabajando en la construcción de ciudades inteligentes, para ello ha diseñado un modelo de medición de la madurez de ciudades y territorios inteligentes en Colombia con el objetivo de identificar oportunidades y prioridades para definir una visión y una hoja de ruta concreta y viable en el proceso de transformación digital.

El modelo propuesto busca medir el estado actual de 61 territorios en torno a 6 componentes: Medio Ambiente, Hábitat, Desarrollo Económico, Personas, Calidad de Vida y Gobernanza, con este análisis se busca identificar la manera en que las ciudades y territorios se están apalancando bajo estas dimensiones con los nuevos habilitadores digitales y como segunda instancia a través de encuestas a la ciudadanía se pretende identificar e integrar al diseño del modelo de Ciudad Inteligente la visión que sus ciudadanos tienen sobre el desarrollo de sus territorios, a fin de construir un modelo plural e incluyente que refleje las opiniones e intereses de sus habitantes (MINTIC, 2020).

Con relación a cada una de las dimensiones propuestas para una ciudad inteligente en el contexto colombiano, son muchos los aspectos que hay que abordar en función del modelo empezando por la dimensión de datos, es importante ver esta dimensión como un habilitador fundamental para el desarrollo tanto del país como de la ciudad que los ciudadanos quieren construir. Se hace necesario crear una plataforma descentralizada que permita la recopilación y administración de los datos digitales de los ciudadanos, convertir estos datos en información

relevante para la toma decisiones e integrar soluciones de gobierno digital a medida que se avanza hacia la digitalización de la ciudad. Para ello es fundamental crear alianzas público-privadas que permitan ofrecer servicios en línea que generen valor a los ciudadanos, pero con métodos seguros de autenticación, adoptando soluciones como la identificación digital que en conjunto con políticas que permitan ampliar la cobertura de internet seguro para todos, a bajos precios y con excelente calidad le permitan al ciudadano disfrutar de los servicios que se pongan a su disposición.

Para la dimensión de Gobierno digital es necesario hacer un esfuerzo importante con proyectos de modernización de la infraestructura tecnológica de las alcaldías, de tal manera que se puedan desplegar una gama amplia de servicios que regularmente implican a los ciudadanos realizar largas filas para pagar los servicios y posteriormente para recibirlos, en este sentido se deben ofrecer servicios enfocados en el bienestar del ciudadano, mejorando la oportunidad en los tiempos de atención. Para ello es necesario hacer esfuerzo enfocados en la integración y estandarización de las plataformas y los diferentes sistemas de información que hoy en día son islas, implementando proyectos de arquitectura empresarial. Estos proyectos de la mano con soluciones de inteligencia de negocio permitirían implementar mejoras en la toma de decisiones.

Para las dimensiones de movilidad, educación, salud y servicios públicos son muchos los proyectos, productos y servicios que desarrollar y poner a disposición de la ciudadanía y sobre cada uno de estos ítems habrá tecnología soportando las soluciones implementadas, sobre todo tecnologías disruptivas ya mencionadas tales como IOT, cloud computing, IA, Big data y BI que traerán consigo retos asociados a la ciberseguridad propios del servicio y la tecnología

11.1 RECOMENDACIONES GENERALES EN EL CONTEXTO DE LA CIBERSEGURIDAD

Los pilares de la seguridad de la información son la disponibilidad, la integridad y la confidencialidad, incluso algunos autores incluyen la autenticación como un cuarto pilar, cuando se quiere evaluar el tema de ciberseguridad a nivel de una ciudad son muchos más los aspectos a considerar para ejercer un control efectivo que permita garantizar a los ciudadanos la privacidad de sus datos directos o indirectos, la prestación de los servicios y la interconexión de los distintos sistemas desplegados.

Para la implementación del modelo propuesto se realizan las siguientes recomendaciones:

- La información del ciudadano debe estar concentrada en una plataforma que tenga el control de los datos que permitan la identificación de las personas tal como nombre, documento de identidad, dirección, correo electrónico y en general cualquier dato que permita conocer quién es el propietario de los datos.
- Los gobiernos al convertirse en el gestor responsable, mas no el propietario, de los datos de los ciudadanos tienen la necesidad y obligación de tratarlos con un enfoque integral basado en riesgo, el cual permitirá que cada dato recolectado dentro de los múltiples sistemas de tecnología asociados a los sistemas públicos, sea considerado como un activo de alto valor. Esto permitirá evaluar de manera más integral, considerar, reducir y mitigar cualquier amenaza que tenga como objetivo la obtención de dichos datos.
- Los gobiernos locales deberán redactar legislación sobre temas de ciberseguridad, protección de datos y de infraestructura, a la medida de las necesidades puntuales de cada territorio y exigir su cumplimiento. Un primer paso para esto será revisar la

regulación existente en otros países que vienen trabajando en estos temas con anterioridad, es importante tener presente que los ataques pueden venir del exterior con el objetivo de atacar la estabilidad del territorio nacional, crear crisis o solicitar dinero por el rescate de la información, una buena referencia sería el reglamento general de protección de datos de la Unión Europea (RGPD) para la protección de los datos de los ciudadanos.

- Implementar soluciones de machine learning que permitan identificar posibles fraudes a través del establecimiento de patrones en las transacciones, de tal manera, que se pueda afrontar el reto de añadir controles específicos de cada contexto, bloqueando solo las transacciones sospechosas en lugar de implantar reglas generales que pueden terminar bloqueando transacciones legítimas. La identificación de patrones aplica tanto para los ciudadanos como para los diferentes dispositivos conectados a las redes debido a que un actor malintencionado podría explotar vulnerabilidades no tratadas, detectando las especificaciones de los aparatos eléctricos y electrónicos dentro de las viviendas de muchas personas, y de esta manera encontrar más modos de atacar otros dispositivos, robando o alterando la información que es transmitida y procesada por los sistemas centrales.
- Cada uno de los componentes tecnológicos provistos por los fabricantes y empresas involucradas en el proyecto, deberá aprobar un proceso de verificación de las mejores prácticas de tratamiento de la información, de vulnerabilidades, actualizaciones y soporte extendido desde la fase de diseño. Debido al alto impacto y alcance que tienen las soluciones de ciudades inteligentes, es recomendado que estas exigencias se implementen como requerimientos de estricto cumplimiento, y no como simples recomendaciones, que pueden ser o no tomadas en cuenta por los fabricantes y demás actores clave.

- Como parte del ciclo de protección de la información e infraestructura tecnológica, es necesario tener constantemente auditorías de firmas independientes, las cuales corroboren y velen por la aplicación de estos lineamientos estrictos de protección de datos e infraestructura tecnológica.
- Uno de los temas a revisar es el desbordamiento de los datos sensibles hacia nubes privadas, transparentes y auditadas, donde se brinden espacios de almacenamiento, protección y cifrado a los datos. Estos servicios de nube no tendrían acceso a ningún tipo de datos de los ciudadanos, y, solamente con la autorización de estos, mediante el uso de algoritmos de cifrados seguros, podrían aprobar o denegar el uso de sus datos. En este modelo, el ciudadano será el único dueño de sus datos, y ni siquiera el gobierno local podrá hacer un uso inadecuado a estos. Implementaciones tales como el cifrado asimétrico de llave pública/privada, podrán ser usados para lograr este objetivo.
- El ciudadano deberá tener control total sobre el ciclo de vida de sus datos, desde su recolección, almacenamiento, procesamiento, borrado y disposición final, de acuerdo con los deberes y responsabilidades como parte activa de una ciudad inteligente. Para ello se deberán implementar servicios de autorización de datos, que le permitirán al ciudadano aprobar o denegar si un componente o actor de una ciudad inteligente como, por ejemplo, una compañía de servicios públicos o una institución de salud podrá tener acceso a sus datos y almacenar más datos dentro de su propiedad.

12. CONCLUSIONES

Luego de finalizar el desarrollo del presente trabajo de grado se puede considerar que se alcanzaron los objetivos propuestos planteados inicialmente y se cumplió el propósito de la investigación. Desde el objetivo de la revisión de literatura en el campo emergentes de las ciudades inteligentes, los estándares y normativas relacionadas con los marcos de ciberseguridad, se evidencia que es un campo de constante desarrollo literario y tecnológico debido a la constante necesidad de implementación en cada una de los territorios con el objetivos de hacerlos más eficientes, con mejores servicios y calidad de vida de sus ciudadanos, por su parte en la revisión de estándares se encontraron varios que combinados logran dar un manejo estratégico a los riesgos que conlleva la inclusión de la tecnología en estos entornos tan amplios en donde es necesario asegurar la integridad, confidencialidad, disponibilidad de la información y la continuidad de los servicios así como evitar ciberataques que atenten contra la infraestructura implementada.

Continuando con el desarrollo de los objetivos planteados, se elaboró un marco de gobierno y gestión que partiendo de los requerimientos funcionales, no funcionales y de dominio, los retos tecnológicos, las dimensiones definidas para la ciudad, los estándares de ciberseguridad, los procesos y proyectos requeridos para el correcto desarrollo de la ciudad, permite visualizar claramente la articulación entre la capa estratégica de la ciudad y la capa estratégica de TI, sin olvidar la estructura organizativa requerida, y complementando el modelo con la administración del desempeño a través de indicadores, seguimiento y control al portafolio de proyectos, la gestión del riesgo, proveedores y equipo de trabajo; finalizando con una capa de mejora continua que garantiza que se van a ir cerrando las brechas entre el estado evaluado y

el estado objetivo, tanto en lo humano, lo tecnológico, los productos, los procesos y la ciberseguridad

Para cerrar se validó el marco de gobierno y gestión de ciberseguridad propuesto en una ciudad genérica del contexto colombiano de categoría I y II, determinando que es totalmente aplicable y conduciría a garantizar que se implementan los controles y estrategias necesarias en torno a la ciberseguridad en cada uno de los contextos en que se desarrolla la ciberseguridad.

13. REFERENCIAS BIBLIOGRÁFICAS

Bayani M., Leiton K. y Loaiza M., (2017). Internet of Things (IoT) Advantages on E-learning in the Smart Cities. *International Journal of Development Research*, 7, (12), 17747-17753.

BBC News. (2017, abril 10). Dallas warning sirens «set off by hacker». *BBC News*. https://www.bbc.com/news/technology-39552471

BBC News Mundo. (2021, mayo 10). EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país. *BBC News Mundo*. https://www.bbc.com/mundo/noticias-internacional-57033536

Behrendt, F. (2016). Why cycling matters for Smart Cities. Internet of Bicycles for Intelligent Transport. Journal of Transport Geography. 56, 157–164

DNP (2018). Departamento Nacional de Planeación. Índice de ciudades modernas de Colombia. Recuperado 9 de junio de 2021, de https://colaboracion.dnp.gov.co/CDT/Vivienda%20Agua%20y%20Desarrollo%20Urbano/SMART%20CITIES/2018/1_Indice%20Ciudades%20Modernos_ACORCHUELO.pdf?

DNP (MARZO 2018). Departamento Nacional de Planeación. Objetivos de desarrollo sostenible. Recuperado 27 de septiembre de 2021, de https://www.ods.gov.co/es/objetivos/

ESET. (2015, junio 16). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

E-Estonia (2021). e-estonia toolkit. Presentation slideshow Recuperado 17 de octubre de 2021, de https://e-estonia.com/wp-content/uploads/e-estonia-200121-es.pdf

Financiera del Desarrollo Territorial SA, F. (2014). *Diamante Caribe y Santanderes*.

Font, T., & Ortega, P. (2019). *PAZ Y CONSTRUCCIÓN DE EN LAS CIUDADES*. 39. http://centredelas.org/wp-content/uploads/2020/06/Informe38_ViolenciaPazCiudades_CAST_web_DEF.pdf

Instituto de Estudios Urbanos (IEU). (2017). *Crecimiento urbano en Colombia: Alcances y restricciones*. http://ieu.unal.edu.co/en/medios/noticias-del-ieu/item/crecimiento-urbano-en-colombia-alcances-y-restricciones

ISO. (2018a). *ISO 37106:2018(en), Sustainable cities and communities—Guidance on establishing smart city operating models for sustainable communities*. https://www.iso.org/obp/ui/#iso:std:iso:37106:ed-1:v1:en

ISO. (2018b). *ISO ISO 37120:2018. Sustainable cities and communities — Indicators for city services and quality of life.* https://www.iso.org/standard/68498.html

ITU (2010). Ciberseguridad. Actualidades de la UIT. vol. 9. Recuperado 19 de junio de 2021, de https://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

ITU (2015). Cybersecurity, data protection and cyber resilience in smart sustainable cities. Recuperado 9 de junio de 2021, de https://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/website/web-fg-ssc-0090-r7-technical_report_on_ICT_infrastructure_for_resilience_security.doc

Kiara. (2021, marzo 24). Todo lo que debes saber sobre seguridad cognitiva. *Kiara*. https://www.kiara-tech.com/todo-lo-que-debes-saber-sobre-seguridad-cognitiva/

Mack, A. (2005). *El concepto de seguridad humana*. Papeles. vol 90. https://www.fuhem.es/media/ecosocial/file/Cohesi%C3%B3n%20Social/Necesidades,%20consumo%20y%20bienestar/MACK,%20Andrew,%20El%20concepto%20de%20seguridad%20humana,%20Papeles%2090.pdf

Ministerio de las tecnologías de la información y las Comunicaciones [MINTIC], Iniciativas. Recuperado 3 de enero de 2022 de *https://www.mintic.gov.co/portal/inicio/Iniciativas/*

Ministerio de las tecnologías de la información y las Comunicaciones [MINTIC], (01 de octubre de 2020). *MinTIC impulsa a 61 ciudades de Colombia para que se conviertan en territorios inteligentes.* Recuperado 15 de noviembre de 2021 de https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/151446:MinTIC-impulsa-a-61-ciudades-de-Colombia-para-que-se-conviertan-en-territorios-inteligentes

NIST. (2018, febrero 8). *NIST Cybersecurity Framework, 2013* [Text]. NIST. https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

Organización para la Cooperación y el Desarrollo Económicos (OCDE). (s. f.). *Tu Índice para una Vida Mejor*. Recuperado 9 de junio de 2021, de http://www.oecdbetterlifeindex.org/es/countries/colombia-es/

Quintero, C. A. (2019). *Informe de las Tendencias del Cibercrimen en Colombia (2019-2020)*. 36. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Rodríguez, V. M. M., Guío, A., Quintero, L. F., Ospino, L. A. R., & Gaviria, D. G. (2020). *Documento de Recomendaciones para el Desarrollo de Ciudades y Territorios Inteligentes*. 68. https://gobiernodigital.mintic.gov.co/692/articles-159996_Recomendaciones_Desarrollo_CI.pdf

Tamayo, M. (2003). El proceso de la investigación científica. Ciudad de México, México: Editorial Llmusa, S.A.

UIT (2014). Las ciudades inteligentes y sostenibles: Un análisis de las definiciones. Recuperado 9 de junio de 2021, de

https://observatorioecuadordigital.mintel.gob.ec/wp-content/uploads/2019/11/TR-Definitions-espanol-1.pdf