TRABAJO FINAL DE GRADO

La Cooperación Descentralizada Sur-Sur como medio para convertir a Córdoba en una Ciudad Cibersegura

Rocío Belén Sacchi

DNI: 41225044

Legajo: RIN01382

Licenciatura en Relaciones Internacionales

A todas las personas que caminaron conmigo hasta ahora, por ayudarme a convertirme en la persona que soy.

Resumen

La transformación de las ciudades en *Smart Cities* trae nuevos cambios que conllevan al desarrollo y el crecimiento de las tecnologías de la información (TI) para incrementar el nivel de vida de las personas que habitan en ella. A su vez, esta transformación trae aparejada nuevos desafíos y vulnerabilidades, como lo son los ataques cibernéticos que infringen los datos de la población y desestabilizan e interrumpen el correcto funcionamiento de las ciudades y atentan contra el bienestar de sus habitantes. Es por eso que el presente trabajo propone el diseño de un plan de internacionalización para la Ciudad de Córdoba, siendo esta indispensable para el desarrollo local, cuyo eje principal del trabajo es el diseño de una política cooperativa con el Distrito de Bogotá a través de la Cooperación Descentralizada Sur-Sur, basada en la prevención y respuesta ante posibles ataques cibernéticos para convertir a Córdoba en una ciudad Cibersegura a través de 3 ejes a consolidar en un lapso temporal de 2 años: 1) consolidar una política de ciberseguridad a través de la captación de recursos y cooperación nacional e internacional con la participación del Distrito de Bogotá y otros actores relevantes, 2) fortalecer la protección de las infraestructuras críticas e infraestructuras de tecnología de la información (TI) de la ciudad y 3) fomentar la capacitación en competencias digitales en el Municipio y la población en general.

El presente trabajo busca la profundización y el pleno desarrollo de la Ciberseguridad en la Municipalidad de Córdoba, a través de la cooperación internacional e interinstitucional, debido a que es un asunto de vital importancia para el correcto funcionamiento de la Ciudad y sus entidades e instituciones, con la finalidad de proteger la seguridad, integridad y bienestar de la población y sus datos. Mejorando las relaciones intersectoriales en el municipio y enriqueciendo las relaciones internacionales con gobiernos no centrales a través del establecimiento de nuevos contactos formales e informales, en vista de posicionar a la ciudad de Córdoba en la materia.

Palabras Claves: Ciudades Inteligentes, Ciberseguridad, Cooperación internacional, Paradiplomacia, Internacionalización.

Abstract

The transformation of cities into Smart Cities brings new changes that lead to the development and growth of information technologies (IT) to increase the quality of life of the people who live there. At the same time, this transformation brings new challenges and

vulnerabilities, such as cyber attacks that infringe on the population's data and destabilize and disrupt the proper functioning of cities and threaten the welfare of its inhabitants. That is why the present work proposes the design of an internationalization plan for the City of Cordoba, being this indispensable for local development, whose main axis of the work is the design of a cooperative policy with the District of Bogota through the South-South Decentralized Cooperation, based on the prevention and response to possible cyber attacks to turn Cordoba into a Cybersafe city through 3 axes to consolidate in a lapse of time of 2 years: Consolidate a cybersecurity policy through the attraction of resources and national and international cooperation with the participation of the District of Bogota and other relevant actors, strengthen the protection of critical infrastructure and information technology (IT) infrastructure of the city and promote training in digital skills in the Municipality and the population in general.

The present work seeks the deepening and full development of Cybersecurity in the Municipality of Córdoba, through international and inter-institutional cooperation, because it is a matter of vital importance for the proper functioning of the City and its entities and institutions, in order to protect the security, integrity and welfare of the population and its data. Improving intersectoral relations in the municipality and enriching international relations with non-central governments through the establishment of new formal and informal contacts, with a view to positioning the city of Córdoba in the matter.

Keywords: Smart Cities, Cybersecurity, International cooperation, Paradiplomacy, Internationalization.

Introducción

A través de la historia, las ciudades se han ido convirtiendo en centros urbanos de intercambio, cooperación y desarrollo para la población. Estos centros fueron creciendo a lo largo del tiempo, aumentando la necesidad de los municipios que los dirigían de adaptarse a nuevas formas de administración. Tal es así, que en la actualidad los gobiernos necesitan plantearse la evolución en la forma de gestionar las ciudades a través de la administración pública y las nuevas tecnologías.

Para ello las tecnologías de la información y las comunicaciones (TIC) se han vuelto indispensables, formándose así el concepto de "Smart City" y naciendo con el mismo nuevas amenazas y vulnerabilidades, las cuales deben ser tratadas de manera urgente desde la "Ciberseguridad".

La Unión Internacional de Comunicaciones propone la siguiente definición de ciberseguridad:

> 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 ciber entorno. (UIT, 2018: Cláusula 3.2.5)

La primera vez que apareció una amenaza importante para la infraestructura global fue a finales de los años 80. Esta amenaza, llamada gusano "Morris", se propagó e infectó rápidamente a sistemas de TI de todo el mundo. Este incidente es el que actuó como detonante y alarma, dando cuenta al mundo que necesitaban de la cooperación y la coordinación entre administradores y gestores de sistemas informáticos para enfrentarse a estas nuevas amenazas, creándose así el primer CSIRT.

Por consiguiente, en el presente trabajo se realiza un Reporte de caso con el propósito de fortalecer la cooperación descentralizada sur-sur entre la Municipalidad de la Ciudad de Córdoba con el Distrito Capital de Bogotá, Colombia; a fin de lograr el fortalecimiento de la seguridad cibernética y el cuidado del funcionamiento del municipio, y proteger el bienestar de la ciudadanía a través de la Ciberseguridad, amparando al proyecto "Smart cities" y contribuyendo para su desarrollo seguro.

Para entender la relevancia de la temática, debemos comprender la problemática identificada; la cual se fundamenta al analizar las alianzas y acciones del Municipio para convertir a la ciudad en una Smart City, destacando por un lado a la gestión realizada por la Secretaría de Planeamiento, Modernización y Relaciones Internacionales para entrar a la Alianza Global de Ciudades Inteligentes del G20 (G20 Global Smart Cities Alliance), en donde Córdoba fue seleccionada para formar parte en el año 2020.

Y por el otro lado la puesta en escena por parte del municipio de los 5 principales ejes de Smart City en la Ciudad, en donde se incluyen la creación del "CorLab" el Laboratorio de Innovación Govtech de la Municipalidad de Córdoba. El eje "Córdoba Ciudad Global" posicionandola como una ciudad abierta al mundo. La creación del Centro de Transformación digital para la transformación y el uso de metodologías ágiles, co-creando soluciones innovadoras, modernas y eficientes a problemas y desafíos públicos, como el Registro Civil Digital, la aplicación Vecino Digital, la app ciudadana, entre otros. El fondo Córdoba Ciudad Inteligente, el cual promueve la inversión en emprendimientos innovadores de alto impacto que generan beneficios positivos para la sociedad, el ambiente y la economía. Y como último eje, el "HUB de Ciberseguridad" que tiene como objetivo posicionar a la ciudad de Córdoba como un polo tecnológico referente en materia de ciberseguridad que brinda productos y servicios de alta calidad a organizaciones públicas y privadas.

Si bien Córdoba cuenta con el HUB de ciberseguridad, sus principales líneas de acción se enfocan en generar mayor conciencia y cultura sobre ciberseguridad en la ciudadanía en general, lo que implica el diseño e implementación de acciones de sensibilización y formación para posicionar en organizaciones públicas, privadas y en la comunidad la importancia de la ciberseguridad, pero este no cuenta con equipos especializados que reaccionen frente a ataques cibernéticos en el sector público o que respondan ante ataques hacia la población en general.

La base de la problemática que aborda el presente reporte de caso, es que se presenta un alto desarrollo en transformación digital y tecnológica para lograr que Córdoba se convierta en una Smart City pero no se plantea esta transformación desde el enfoque de la ciberseguridad, generando un alto volúmen de datos que ponen como blanco de ciberataques a la ciudad, a sus instituciones y sus habitantes.

Por esta razón, se puede inferir que existe una oportunidad de mejora para proteger a la ciudad y a quienes habiten en ella a través de la cooperación sur-sur, en donde se busca que Córdoba logre instalar un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), siendo este:

> Un equipo de expertos en Seguridad de Tecnologías de la Información (TI) que responde a amenazas o incidentes de la seguridad de la información. Los CSIRT tienen la capacidad y competencia para detectar y manejar estos incidentes y/o amenazas, así como también de ayudar a sus miembros a recuperarse de estos ataques. De forma proactiva un CSIRT puede ofrecer diversos servicios con la finalidad de mitigar vulnerabilidades y riesgos, hacer conciencia y educar a sus miembros con el desarrollo y mejora de los servicios de seguridad de ellos. (van der Heide, 2020, p.4)

Sea así la principal función de este centro, realizar un plan de identificación de activos críticos de la ciudad, donde se establezcan áreas de vulnerabilidad en el funcionamiento de los sistemas y en la recolección y utilización de datos, con el fin de reaccionar acertadamente y con los protocolos adecuados en caso de enfrentar ataques cibernéticos que puedan atentar contra la operatividad de la ciudad y a su vez, se dedique a concientizar y brindar asistencia a funcionarios municipales.

Resulta de gran interés el accionar del Banco Interamericano de Desarrollo; “El BID es la principal fuente de financiamiento y pericia multilateral para el desarrollo económico, social e institucional sostenible de América Latina y el Caribe.” (Banco Interamericano de Desarrollo [BID], s.f.); prioriza la inclusión social, la igualdad, la innovación, la productividad y la integración regional.

Esta organización ha publicado una “Guía de Ciberseguridad para Ciudades Inteligentes” en donde al ser una entidad de tal consideración, es importante tener en cuenta la magnitud de una guía publicada por este organismo. Esta guía tiene como objetivo proporcionar una serie de conocimientos que permitan comprender y analizar la seguridad cibernética y su importancia para el correcto funcionamiento de las ciudades de América Latina y el Caribe; entendiendo los riesgos, los potenciales impactos y la necesidad de actuar con urgencia y de manera proactiva para proteger a las ciudades y a quienes habitan en ellas; de modo que sirva a líderes locales, gerentes, empleados municipales y al personal técnico en Tecnologías de la Información y Comunicación (TIC), para fortalecer la digitalización, reducir las posibilidades de futuros ciberataques y al mismo tiempo saber reaccionar en caso de que la seguridad cibernética y los sistemas hayan sido vulnerados.

El marco de referencia institucional se encuentra compuesto por el análisis de los actores involucrados en nuestra investigación. Identificando a la Municipalidad de Córdoba,

específicamente la Secretaría de Planeamiento, Modernización y Relaciones Internacionales en el interior de la estructura de la Municipalidad de Córdoba, siendo la secretaría encargada de la dirección de los proyectos ya existentes en la temática como el Hub de Ciberseguridad y de las operaciones para la internacionalización de la ciudad, en nuestro caso con el fin de posicionarla en materia de ciberseguridad y estrechar lazos con la ciudad colombiana.

Por otra parte, se trabajará en conjunto con el Distrito Capital de Bogotá por medio del sector de Gestión pública mediante la Alta Consejería TIC quien se encarga de lograr una ciudad moderna con un modelo de gobierno abierto, contribuir a la construcción de la paz y la reconciliación, y mejorar la calidad de vida de la ciudadanía y la Dirección Distrital de Relaciones Internacionales (DDRI), la cual busca la internacionalización de la ciudad a través de alianzas internacionales y eventos que posicionan a la ciudad en el mundo, colaborando así con la Alta Consejería TIC mediante la cooperación con organizaciones y países y el financiamiento exterior.

Bogotá ha estado realizando varios avances en ciberseguridad los cuales la han posicionado en la materia en relación a otras ciudades de Latinoamérica. Se ha implementado un plan de articulación institucional, alianzas estratégicas y programas de capacitación que han dado resultados positivos.

También destacar la importancia sobre que a nivel país Colombia obtuvo el mayor desarrollo en seguridad cibernética en LatAM, según el Observatorio de Ciberseguridad en América Latina y el Caribe en un estudio realizado por el Banco Interamericano de Desarrollo y la OEA, particularmente en las dimensiones “Política y estrategia” y “Cultura y sociedad”.

Con la finalidad de descubrir antecedentes relevantes para la aplicación de proyectos de ciberseguridad en la ciudad de Córdoba, la investigación utilizará una herramienta llamada benchmarking identificándose como: “el benchmarking es un proceso sistemático y continuo para evaluar los productos, servicios y procesos de trabajo de las organizaciones que son reconocidas como representantes de las mejores prácticas, con el propósito de realizar mejoras organizacionales” (Spendolini, 2005, p. 2).

En primer lugar, se analiza a la ciudad de Buenos Aires, la cual en el año 2017 inauguró el primer centro de expertos en ciberseguridad en América Latina llamado “BA-CSirt”, siendo pioneros de un centro de especialistas en la materia que se dedica a concientizar y brindar asistencia al propio gobierno y a la ciudadanía, mejorando su posición a nivel LatAm y funcionando como referentes para quienes necesiten acudir para capacitarse, informarse o pedir ayuda ante incidentes; brindando una respuesta rápida y eficiente en

momentos de vulnerabilidad y/o amenazas. Dentro de sus capacidades es posible reportar incidentes y resguardar evidencia, informarse acerca de propuestas educativas y concientizarse, realizando cursos, talleres y charlas sobre la temática. También se brinda asesoramiento en casos que no son estrictamente incidentes, informando sobre tecnología y ciberseguridad, resguardando a la población.

Otro caso de referencia es el Grupo de Respuesta a Incidentes de Seguridad Bahía/Brasil (CERT.Bahía), cuya función es coordinar y actuar en relación a la prevención y el tratamiento de incidentes de ciberseguridad en instituciones conectadas al Punto de Presencia de RNP en Bahía y en las instituciones socias de la Red Metropolitana de Salvador (ReMeSSA). Busca ser un grupo que contribuya a la comunidad con el fin de reducir el número de incidentes de seguridad y mejorar las tecnologías de prevención y tratamiento. Actúa coordinando a las instituciones en un proceso de respuesta a incidentes de seguridad, facilitando el intercambio de información y cooperación entre las partes involucradas. A su vez, brinda orientación a instituciones para que puedan manejar incidentes de manera correcta y divulga información sobre ataques, vulnerabilidades y amenazas a la seguridad junto con recomendaciones sobre cómo abordar y prevenir los problemas.

Como último antecedente, el Laboratorio de Datos y Sociedad es un proyecto que reúne a un equipo de profesionales que buscan la promoción de un marco de referencia sobre los derechos humanos en la era digital de Uruguay, impulsado por un proyecto de la sociedad civil llamado DATA Uruguay. Desde 2016, se trabajó sobre la vigilancia de la privacidad, las comunicaciones y la ciberseguridad en Uruguay. Realizaron un mapeo de la situación, conceptualizando el impacto que podría tener una serie de normas en los delitos informáticos a partir de los derechos humanos; desarrollaron acciones de capacitación, sensibilización y autodefensa digital para organizaciones, periodistas y defensores de los Derechos Humanos; realizaron acciones para fomentar la discusión y la formación en relación a internet y los DDHH.

En el 2020 con ayuda de la Iniciativa por los derechos digitales en Latinoamérica (INDELA) quien financia, capacita y brinda apoyo a organizaciones que promueven los derechos digitales en Latinoamérica, se buscó fortalecer la agenda de derechos digitales en Uruguay, impulsando espacios de cooperación entre el sector privado y el público y producir conocimientos en la temática.

En la actualidad, si bien se inauguró un HUB de Ciberseguridad, la Ciudad de Córdoba no cuenta con un equipo de respuesta ante incidentes de seguridad informática como lo hacen estos actores, por lo que la Ciudad y su población se encuentra expuesta a la

vulnerabilidad de sus redes y sistemas y a la posibilidad de ser víctimas de ciberataques que afecten el correcto funcionamiento de la ciudad, la seguridad de sus habitantes y la divulgación de datos sujetos a la privacidad.

Análisis de situación

Descripción de la situación:

Para dimensionar el tamaño y la importancia de la Ciudad de Córdoba, a nivel provincia el 40,18% de la población está aglomerada en la capital provincial, con 1.329.604 de habitantes, siendo así la segunda aglomeración urbana del país (Municipalidad de Córdoba, s.f.).

El nacimiento de la Secretaría de Planeamiento, Modernización y Relaciones Internacionales, surge con la llegada de Martin Llaryora como nuevo intendente de la Municipalidad de Córdoba. Ésta nueva área trabaja conjuntamente en brindar soluciones innovadoras y estratégicas en un contexto internacional que se actualiza y muta constantemente.

Estos objetivos se ordenan y persiguen a través de una serie de lineamientos, siendo relevantes para el plan dos de los ejes estratégicos del Plan de Metas 2020-2023 de la Municipalidad, en donde se destaca que:

El Plan de Metas de Gobierno se instituye como un instrumento de planificación e información ciudadana, a través del cual el Poder Ejecutivo presenta su programa de gestión y da a conocer los lineamientos que guiarán la actividad de la administración pública municipal durante el período de gobierno. (Plan de Metas de Gobierno, 2020, p.7)

Córdoba busca a través del eje número uno del Plan de Metas de Gobierno, convertirse en un Municipio moderno e innovador, que logre atender las demandas de una ciudadanía con carácter activo y responsable, procurando mejorar el feedback con la misma mediante la sistematización y digitalización para una administración más accesible, abierta, transparente y despapelizada, a través de mecanismos como la identidad digital, las notificaciones electrónicas, la interoperatividad entre las bases de datos, audiencias públicas

digitales, entre otras, que permiten el aumento de la eficiencia de los recursos públicos mediante la tecnología.

En relación al eje número tres del Plan de Metas de Gobierno, como una ciudad atractiva y planificada; uno de lineamientos a seguir es la transformación en una ciudad abierta al mundo, participando en la agenda global y en redes de internacionalización en la búsqueda de oportunidades para el desarrollo local, con innovaciones en la captación de inversiones, fortaleciendo la innovación y el emprendedorismo y articulando alianzas y cooperación público-privadas.

A través de este plan moderno e innovador, Córdoba busca implementar nuevas estrategias y soluciones para mejorar el bienestar de sus ciudadanos y aumentar la eficiencia de los servicios públicos. Una de las herramientas para perseguir las metas y objetivos nombradas en el Plan de Metas de la ciudad es la transformación de la ciudad en una Smart City a través de la Secretaría de Planeamiento, Modernización y Relaciones Internacionales, la cual siguiendo la definición de Bouskela et al. (2016):

> Una “Smart City” o ciudad inteligente, es aquella que coloca a las personas en el centro del desarrollo, incorpora Tecnologías de la Información y Comunicación (TICs) en la gestión urbana y usa estos elementos como herramientas para la formación de un gobierno eficiente que incluya procesos de planificación colaborativa y participación ciudadana. Al promover un desarrollo integrado y sostenible, las Ciudades Inteligentes se tornan más innovadoras, competitivas, atractivas y resilientes, lo cual contribuye a mejorar las vidas de sus habitantes.

Logrando como resultado la adaptación de las TICs a sectores como infraestructura, energía, transporte, saneamiento, educación, salud, vivienda y empleo.

En el contexto de las "ciudades inteligentes" o "Smart Cities", la gestión urbana y la adaptación de las Tecnologías de la Información y la Comunicación (TIC) a diversos sectores están estrechamente relacionadas. Las ciudades inteligentes utilizan las TIC para recopilar y analizar datos en tiempo real sobre distintas áreas, y con esta información toman decisiones informadas para mejorar la eficiencia en la gestión de servicios públicos, la planificación urbana y la toma de decisiones. Por tanto, la gestión urbana y la adaptación de las TIC a diversos sectores públicos buscan crear ciudades más inteligentes y sostenibles, capaces de adaptarse y responder eficazmente a los cambios y desafíos del entorno urbano.

Sin embargo, los avances y el crecimiento vienen de la mano de nuevos riesgos y amenazas. Las ciudades inteligentes utilizan cada vez más el ciberespacio, siendo este "...una compleja infraestructura de redes de conectividad e interfaces de comunicación, de sensores y dispositivos conectados, de centros de operación y control. (Cotino y Sánchez, 2021, p. 6)

Este moderno modelo de ciudades contiene nuevos elementos que se vuelven importantes a la hora de definir las debilidades y amenazas que poseen los municipios, en consecuencia, el nuevo contexto internacional obliga a que ciudades como Córdoba a través del municipio tomen las medidas necesarias para actuar en contra de las nuevos peligros que vienen de la mano de los avances en las TIC mediante la Ciberseguridad.

Como resultado de los procesos de transformación digital, la interconectividad y el masivo uso de datos, se podrían provocar estragos a la hora de sufrir ataques cibernéticos, resultando de suma importancia reconocer la necesidad de contar con un área que trate los temas relacionados a la ciberseguridad, previniendo amenazas y sabiendo cómo actuar en caso de que estas se materialicen; evitando gastos adicionales una vez que el sistema esté en funcionamiento, ya que la interrupción de servicios públicos y/o la intermisión de la infraestructura de la ciudad podrían ocasionar altos costos sociales, políticos, económicos y reputacionales que ponen en peligro el bienestar de la población.

Es por eso que Mckinsey, una consultora estratégica global que se focaliza en resolver problemas concernientes a la administración estratégica, afirma:

> La seguridad cibernética desempeña un rol crítico en la mitigación de impactos y tensiones al proteger la confidencialidad, integridad y disponibilidad de los datos y la infraestructura habilitada para datos. Sin embargo, la seguridad por sí sola no es suficiente. La ciber resiliencia va un paso más allá al garantizar que los sistemas de tecnología de la información y las comunicaciones (TICs) sigan ofreciendo servicios en caso de un incidente cibernético. (McKinsey, 2018, parr. 2)

Es debido a la gran importancia de la ciber resiliencia que se debe comprender a través de su capacidad de preparación, respuesta y reinvención.

Enfocándonos en la conexión y el contexto entre ambas ciudades, para que Córdoba y Bogotá puedan llevar a cabo la cooperación, debemos tener en cuenta que son partes de la Alianza del G20 de Smart cities, y su conexión se acentúa dentro de la *LatAm Smart Cities Alliance*, las cuales cuentan con el apoyo del Foro Económico Mundial a través del equipo

dedicado del C4IR Colombia, cuyo fin es participar y cooperar con grupos de trabajo conformados por expertos en políticas para desarrollar nuevas políticas en materia de ciudades inteligentes y unirse a la Red de Apoyo para lograr la ayuda mutua entre las ciudades de LatAm que participan de la Alianza e implementar mejores políticas público-privadas; encontrándose también en la hoja de ruta de políticas modelo un apartado llamado Política de rendición de cuentas de ciberseguridad que trata temas importantes para el desarrollo de ciberseguridad de las ciudades involucradas en la alianza.

Análisis del contexto:

Análisis político:

En relación al artículo 4 de la Carta Orgánica de la Municipalidad de Córdoba (1995) se establece que la ciudad organiza sus instituciones bajo la forma representativa, republicana, democrática y participativa.

En la actualidad se encuentra ejerciendo la intendencia de la Ciudad de Córdoba el Intendente Martín Llaryora, perteneciente al Partido Justicialista al igual que el Gobernador Juan Schiaretti, quien ejerce la gobernación de la provincia, lo que permite un mayor consenso y cooperación al momento de perseguir objetivos y realizar acciones conjuntas. En relación al poder nacional, si bien Córdoba pertenece al mismo movimiento partidario que la presidencia, se han conformado discrepancias y problemas a la hora de llegar a consensos políticos y en materia presupuestaria, dificultando la continuidad en la toma de decisiones.

Análisis tecnológico:

Respecto al análisis tecnológico, en primer lugar, hay que destacar el importante trabajo que han realizado desde la Municipalidad de Córdoba en función de que la ciudad se convierta en una Smart City, uniendo en sus acciones a los campos más importantes de la actualidad, la internacionalidad, la innovación y las nuevas tecnologías, a fin de brindarle un mayor bienestar a toda la población.

En consiguiente y gracias a estos esfuerzos, Córdoba ya comenzó a trabajar en la problemática de Ciber seguridad, si bien sus actividades son recientes la ciudad ha podido dar sus primeros pasos a través del lanzamiento del Córdoba Cyber-Security HUB coordinado desde la Secretaría de Planeamiento, Modernización y Relaciones Internacionales de la

Municipalidad, el cual busca posicionar a la ciudad como polo tecnológico en ciberseguridad logrando la cooperación entre organizaciones públicas y privadas, emprendedores, instituciones referentes, académicos y empresarios.

Como uno de los principales objetivos del Hub, han realizado la publicación “Oferta educativa sobre la ciberseguridad en la Ciudad de Córdoba”, con el fin de formar nuevos talentos especializados en seguridad informática, siendo “... un documento que concentra la oferta educativa en ciberseguridad que brindan las Universidades de la ciudad de Córdoba para facilitar el acceso a la formación de quienes se interesen en este sector” (Municipalidad de Córdoba, 2022). A su vez, se distingue el “1er Congreso de Ciberseguridad, desde Córdoba Capital para toda la Región” en el año 2022, el cual marca un hito en la ciudad para el sector tecnológico y de la ciberseguridad, con el objetivo de generar mayor conocimiento y cultura sobre ciberseguridad en el sector privado y público y en la ciudadanía en general. El mismo contó con una conferencia plenaria y con paneles diversos en donde especialistas abordaron diferentes ejes relacionados a la ciberseguridad.

Finalmente, la MC cuenta con CorLab, el Laboratorio de Innovación GovTech de la Municipalidad de Córdoba, cuyo fin es promover la articulación público-privada y acelerar los procesos de innovación en la ciudad. Éste espacio funciona como un sistema de apoyo transversal para gestionar la innovación y la transformación digital en otras áreas de Gobierno, trabajando y cooperando con Organismos Multilaterales, Organizaciones sociales, Universidades y emprendedores, bajo un modelo de innovación abierta, donde se co-crean soluciones innovadoras con un gran impacto social, económico y ambiental. Tal es así que permite experimentar nuevas formas de generar valor público, aportar nuevos canales de participación, potenciar la relación con la ciudadanía y colaborar con nuevas metodologías de trabajo más eficientes.

En consecuencia, se implementaron nuevos adelantos en relación al uso de tecnologías y la digitalización del Municipio. Se crearon nuevas aplicaciones, se puso en funcionamiento el uso de la identidad digital a través de la plataforma de Vecino Digital, la posibilidad de realizar una gran cantidad de trámites de forma digital, entre otros.

Es por estas cuestiones que el proyecto toma gran importancia en relación a la protección de estos nuevos datos que ingresan al sistema, siendo una gran amenaza que tales sean vulnerados por ataques cibernéticos, ayudándonos a entender la relevancia de contar con un centro de expertos en ciberseguridad que proteja a la población y a estos grandes avances que trae la MC.

Análisis legal:

En cuanto al contexto legal en materia de modernización e innovación se decidió establecer una alianza estratégica con el Gobierno de la provincia de Córdoba, así en sus primeros días de gestión, el Municipio a partir de la Ordenanza 12.985/2020 se adhirió a la Ley Provincial N° 10.618/2019 de Simplificación y Modernización de la Administración Pública y, a su vez, al Decreto 1280/2014 de Ciudadano Digital, denominado CiDi. Definiendo el rumbo de la administración pública hacia el objetivo de un gobierno digital y electrónico.

En materia de ciberseguridad y el ámbito legal, Córdoba no cuenta con ordenanzas municipales ni provinciales que legislen en la materia, y pese a la mínima legislación que existe en materia de ciberseguridad y ciberataques, se destacan por un lado a nivel nacional la Ley 25.326 de Protección de Datos Personales, la cual en conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional, tiene por objeto la protección integral de los datos personales recogidos en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. Ley 25.326. Ley de Protección de Datos Personales. Art. 43 (2000)

Por otro lado, el marco normativo vigente de la República Argentina en materia de delitos informáticos, evidencia que ha sido modificada la Ley 26.388 sobre Delitos Informáticos, modificando el Código Penal Argentino e incorporando una serie de Delitos informáticos. Entre ellos el delito de hacking, el cual es el caso de mero acceso no autorizado a cualquier dato o sistema de acceso restringido, y el cracking, para el caso se haya accedido sin autorización al sistema y se haya modificado, alterado o suprimido cualquier dato del sistema. Es decir, existe sanción penal para los casos de acceso no autorizado a datos o sistemas restringidos, pero puede afirmarse que a pesar de que pueden ser penalmente perseguidos gracias a la legislación penal que los reconoce, se debe resaltar que aunque las víctimas sean datos o sistemas gubernamentales, al momento no existen sentencias que sancionan penalmente a estos hechos.

Análisis económico:

La ciudad de Córdoba se caracteriza por ser polo universitario e industrial. Su PBI en el año 2019 fue de 122.816 millones de pesos corrientes y se encuentra integrado en un 75% por el sector de servicios y en un 25%, por la producción de bienes. Cuenta con siete parques para la radicación de empresas, una importante industria automotriz calificada, producción de software, desarrollo comercial y turístico. (Municipalidad de Córdoba, 2019).

En relación a las fuentes de financiamiento, el presupuesto asignado a la Secretaría de Planeamiento, Modernización y Relaciones Internacionales para el ejercicio de sus actividades en 2022, cuenta con un total de $470.633.180,87, repartido según la naturaleza de sus actividades y la unidad que las ejecuta (Ordenanza N° 13221, p. 463).

A nivel nacional, la Ciudad de Córdoba se encuentra en una situación de inestabilidad económica y política, lo que dificulta el consenso con la Nación y genera dificultades a la hora de definir el presupuesto y el plan de acción.

Análisis social:

A nivel demográfico, Córdoba es la segunda ciudad del país con aproximadamente 1.446.201 habitantes en 2019 con base en los datos proporcionados por el Instituto Nacional de Estadísticas y Censos (INDEC), desplegados en 576 kilómetros cuadrados de territorio y es considerada una de las ciudades más grandes de Latinoamérica con 505 barrios. Según las categorías establecidas por Ciudades y Gobiernos Unidos (CGLU), es una ciudad intermedia en franco desarrollo hacia su metropolización. En la extensa urbe, la co-gobernanza es un aspecto fundamental. Por eso, 13 Centros de Participación Comunal (CPC) descentralizan el poder municipal, donde los vecinos llevan a cabo trámites y requerimientos más cerca de su hogar. (Municipalidad de Córdoba, 2019).

Tal es la importancia del tamaño de la ciudad y la asombrosa cantidad de habitantes, que es de suma relevancia entender la necesidad de que a través de un centro de expertos puedan preverse posibles ataques hacia una urbe tan grande como lo es Córdoba y que, en caso de que estos sucedan, contar con una rápida capacidad de respuesta, por ejemplo, en una situación en la que se afectara a través de un ataque cibernético al sistema de datos de la población recolectados por el municipio. Es vital entender la magnitud de estos tipos de

ataques hacia una ciudad tan importante y la cual cuenta con un flujo y almacenamiento de datos enorme que podría poner en peligro el bienestar de la población.

Diagnóstico organizacional - Análisis F.O.D.A.:

Cuadro N°1

Matriz de Análisis F.O.D.A.

FORTALEZAS **F**	• Córdoba es la segunda ciudad más grande de Argentina. • Se destaca que la ciudad de Bogotá se ha posicionado rápidamente alrededor de ciudades inteligentes y ciberseguridad, por lo que nos brinda una base sólida de cooperación y de lineamientos a seguir para que la MC aumente sus capacidades de respuesta y prevención. • Córdoba ya cuenta con antecedentes en la temática, como lo es el Hub de ciberseguridad y el CorLab, los cuales ayudan a posicionar a la ciudad y brindan capacitaciones a diferentes sectores. • Alto nivel de institucionalización de las Relaciones Internacionales de la MC. • Interés y voluntad política en la temática.
OPORTUNIDADES **O**	• Posibilidades de cooperación con una ciudad posicionada en materia de ciberseguridad y ciudades inteligentes. • Mejorar capacidades de defensa en el ciberespacio que abarca el tejido y la responsabilidad municipal. • Mejorar el posicionamiento de la ciudad siendo una de las pioneras en la creación de centros de expertos en ciberseguridad. • Elaborar políticas públicas y centralizadas en una temática con poco abordaje y gran importancia. • Forjar lazos que posibiliten futuros proyectos conjuntos. • Reducción de las distancias gracias a los avances en telecomunicaciones. • Cooperación con otras áreas de la municipalidad. • Mejorar la seguridad y el manejo de datos • Limitación de las pérdidas que causa la delincuencia cibernética.
DEBILIDADES **D**	• Lento desarrollo legislativo. • Falta de sistematización de la información al ser un área relativamente nueva para la administración pública. • Mínima base de datos. • Desconocimiento del tema y falta de capacitaciones en la administración pública, empresas y en la población en general. • Falta de coordinación entre jurisdicciones. • Riesgo de sufrir ciberataques en las infraestructuras físicas que logren afectar e interrumpir los servicios esenciales. • Escasa participación en el presupuesto municipal.
AMENAZAS **A**	• Tendencia a no ser establecida como una temática prioritaria. • Inestabilidad económica. • Escasez de recursos humanos calificados en ciberseguridad. • Alto desarrollo de aplicaciones sin criterios de ciberseguridad.

Fuente: Elaboración propia.

A raíz de los resultados del análisis FODA, se intentará aprovechar las fortalezas de la ciudad y las oportunidades que el contexto brinda para combatir las debilidades que presenta el Municipio, considerando a su vez, las amenazas que pudieran encontrarse a lo largo del proyecto.

Marco Teórico

En la actualidad, ya no son únicamente los Estados los actores exclusivos en el ámbito de las relaciones internacionales; el alcance se ha desplazado y permitió la emergencia de actores subnacionales quienes en el último tiempo han adquirido una gran relevancia.

Tal es así, que se destacan conceptos como la *paradiplomacia*, definida por Noé Cornago (1999) como:

> La implicación de los gobiernos no-centrales en las relaciones internacionales a través del establecimiento de contactos formales e informales, permanentes o ad hoc con entidades extranjeras, públicas o privadas, con el propósito de promover asuntos de carácter socioeconómicos, políticos o culturales, así como cualquier otra dimensión externa de sus competencias constitucionales. (p. 40)

La paradiplomacia puede ser una herramienta efectiva para abordar los desafíos de seguridad cibernética a nivel local y regional aplicando diversas estrategias.

En primer lugar, la cooperación interregional puede ser fomentada mediante la paradiplomacia, promoviendo la colaboración entre diferentes ciudades y regiones para combatir el crimen cibernético a través del intercambio de información y buenas prácticas, y el desarrollo conjunto de soluciones. En segundo lugar, el desarrollo de políticas regionales permite a los gobiernos subnacionales desarrollar políticas y estrategias de seguridad cibernética adaptadas a las necesidades y circunstancias específicas de su región. Por último, la participación en la toma de decisiones globales permite a los gobiernos subnacionales tener un papel activo en la toma de decisiones globales sobre la ciberseguridad al participar en redes internacionales de ciudades y/o regiones. Esto permite que los gobiernos subnacionales sean considerados en el ámbito internacional y aborden necesidades y preocupaciones relacionadas con la seguridad cibernética junto a otros gobiernos subnacionales que enfrentan los mismos desafíos.

La cooperación internacional entre dos municipios es efectuada a causa de la presencia de dos ciudades de diferentes países que tienen problemáticas similares, en donde deciden cooperar de forma que resulte beneficiosa para ambos actores. “La existencia de valores y percepciones comunes entre los especialistas y los responsables de diferentes administraciones regionales, sobre el diagnóstico y la forma de abordar los problemas del

desarrollo regional." (Cornago, N., 2010), favorecen a la emergencia de la cooperación, enfatizando en la importancia de intercambiar información y experiencias.

Tal es así, que nuestro proyecto busca articular a dos gobiernos sub-nacionales para la ejecución de proyectos y actividades mediante una *Cooperación Sur-Sur*, la cual se remonta a la década de los ´60 y ´70 en donde se constituyó por un vínculo que destacaba la "identidad común" entre los países del tercer mundo, basada en la historia de vínculos coloniales y los problemas de desarrollo. En la actualidad y en ausencia de una definición completamente satisfactoria, una posible formulación es la dada por la Unidad de Cooperación Sur-Sur del PNUD, la cual establece que se trata de un proceso en el que dos o más países en desarrollo pueden adquirir capacidades que van desde lo individual a lo colectivo a través del intercambio cooperativo de conocimientos, recursos y know how tecnológico. (Pino, 2009). Aludiendo a la transferencia de capacidades técnicas y administrativas de forma horizontal, orientándose a la realización de actividades conjuntas que permitan un desarrollo integral.

De forma antagonista, otras autoras han afirmado lo siguiente:

> "...las iniciativas son pequeñas, concretas, sin vinculación con grandes programas de cooperación. Este detalle que parece, a primera vista, sólo una cuestión de escala incide, sin embargo, en su capacidad de adaptación respecto de las políticas locales. La CSS no intenta cambios radicales pero logra insertarse en espacios estratégicos articulándose, necesariamente, con las políticas nacionales. Su envergadura limitada la obliga, por un lado, a un actuar más flexible y le inhibe, por el otro, la capacidad para autonomizarse de la política local. (Kern y Weisstaub, 2011, p.5)

Según el Programa Iberoamericano para el Fortalecimiento de la Cooperación Sur Sur (2011) la existencia de realidades similares favorece el entendimiento, permite el aprendizaje mutuo y alienta a una relación de reciprocidad al compartir modelos de gestión. Utilizando todo tipo de recursos de forma eficaz, racional y solidaria que permiten compartir y disminuir los costos, fortaleciendo las capacidades de gestión en los procesos de cooperación internacional.

En la actualidad las sociedades dependen profundamente de los sistemas informáticos en sectores importantes para la población como los bancos, las instalaciones de energía, el transporte, los datos del gobierno y la ciudadanía, etc. y el enfoque de la comunidad internacional ha aumentado considerablemente frente al espacio cibernético, siendo este "un dominio artificial que se diferencia de los otros cuatros dominios de guerra (tierra, aire, mar y

espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa." (Carlini, A., 2016). Según (Carlini, 2010) los ciberataques han llamado la atención de políticos, agencias de seguridad, empresas privadas y de la población. La existencia del hecho de que se utilice la red para infringir daños preocupa a la Comunidad Internacional, tal es así que es necesario buscar medidas y adaptarse para poder protegerse.

La problemática abordada en el presente trabajo se basa en las capacidades de *ciberseguridad* y el poder que tienen los gobiernos locales para prevenir, reaccionar y enfrentarse a ataques cibernéticos en un contexto en el que las *ciudades inteligentes* se han vuelto de vital importancia para el desarrollo de las urbes, siendo aquellas las cuales insertan a las Tic´s en la gobernanza, incluyen procesos de participación ciudadana y planificación colaborativa y promueven un desarrollo integrado y sostenible, volviéndose innovadoras, resilientes y competitivas, colaborando para mejorar la calidad de vida de sus residentes. Colocan a las personas en el centro del desarrollo y utilizan estos elementos para formar un gobierno eficiente. (Bouskela et al., 2016)

Las Ciudades Inteligentes basan su funcionamiento en un Sistema de Información a través de la recolección de datos e información para un funcionamiento tecnológico e inteligente en distintas áreas de la Ciudad, los cuales a su vez traen aparejados nuevas amenazas y vulnerabilidades que deben ser tratadas desde la ciberseguridad, comprendiendo a ésta 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 ciber entorno. (Unión Internacional de Comunicaciones, 2018: Cláusula 3.2.5)

Las organizaciones y gobiernos entendieron que, si fallan los mecanismos de protección, es sumamente importante contar con estructuras y personal especializado que restablezca los sistemas lo más rápido posible y que maneje los incidentes de seguridad de la información (Georgia, 2003). Es por eso que en el presente trabajo la Municipalidad de Córdoba a través de un proyecto de cooperación con Bogotá busca instalar un centro

denominado “CSIRT” para prevenir y proteger a la población de ciberataques, el cual se compone de:

> Un equipo de expertos en seguridad de TI que responde a amenazas o incidentes de seguridad de la información. Los CSIRT tienen la capacidad y competencia para detectar y manejar estos incidentes y/o amenazas así como de ayudar a sus miembros a recuperarse de estos ataques. De forma proactiva un CSIRT puede ofrecer diversos servicios con la finalidad de mitigar vulnerabilidades y riesgos, hacer conciencia y educar a sus miembros con el desarrollo y mejora de los servicios de seguridad de ellos. (van der Heide, 2020, p.4)

En contraposición de las ventajas que brinda un centro de respuesta, según (Carozo, et al., 2008) podemos encontrar que dentro de las principales restricciones del modelo se observa la dificultad para establecer una comunicación efectiva con toda la comunidad y sus organizaciones y entidades y la posibilidad de ganarse su confianza, siendo necesario que éstas reporten los incidentes y que las recomendaciones de prevención tengan una respuesta positiva y sean continuas, ya que los coordinadores de los centros no tienen una autoridad formal ni la capacidad de forzar a las entidades a cumplir con las recomendaciones ni siquiera en situaciones de grandes ataques, sino que deben actuar en la comunidad realizando recomendaciones y aconsejando a la población, siendo que los miembros de la comunidad pueden elegir no seguirlas.

También es posible que se manejen los incidentes de forma autónoma sin reportarlo al CSIRT, limitando la información que éste recibe y así a su vez su capacidad para determinar el alcance, la naturaleza y el impacto de incidentes.

Diagnóstico y discusión

La llegada de un nuevo gobierno en la Municipalidad de Córdoba en 2019, vino acompañada de una nueva visión política diferente respecto a cuestiones de gestión pública y administrativa en la ciudad, enfocada en la modernización y en la innovación tecnológica.
Abordando una nueva estructura para el área de Planeamiento, Modernización y Relaciones Internacionales, planteando objetivos para convertir a la Ciudad de Córdoba en una Ciudad

Inteligente, aplicando las TIC´s para mejorar la calidad de vida de sus residentes y la accesibilidad, a través de la integración de infraestructuras con sistemas de gestión inteligente.

Desafortunadamente, las vulnerabilidades de los sistemas y datos utilizados en las Smart Cities despiertan la posibilidad de que las infraestructuras físicas sean víctimas de posibles ciberataques que logren afectar e interrumpir los servicios esenciales para millones de personas o vulnerar la recolección de sus datos personales (Atkinson, Castro, Ezell y McQuinn, 2016), ya que las Smart Cities cuentan con una superficie vulnerable a los ataques de enorme tamaño y desconocida por su interdependencia y complejidad.

El gobierno de la ciudad necesita identificar cuáles son sus áreas críticas las cuales necesitan mayor protección frente a diversos tipos de amenazas, ya que puede sufrir incidentes de ciberseguridad cuyo impacto no solo afecta al Municipio sino también a organizaciones dentro del Municipio, a los residentes y a las empresas.

En consecuencia, a continuación, se presentarán una serie de ejes interrelacionados que componen los principales puntos de agenda que Córdoba necesita fortalecer en el área:

A. Débil prevención y capacidad de respuesta ante ataques cibernéticos. Si bien como se nombra con anterioridad Córdoba cuenta con un Hub de ciberseguridad, pero este pone mayor énfasis en la oferta educativa de la ciudad en la materia y en dar visibilidad internacional y no en la respuesta ante las posibilidades de ataques cibernéticos. Siendo innegable la necesidad de contar con un equipo especializado que proteja el bienestar de la población.

B. Escasez de recursos humanos calificados. Este segundo eje está ineludiblemente ligado al primero. La falta de personal capacitado dificulta la prevención de posibles ataques y a su vez la capacidad para reaccionar frente a amenazas cibernéticas. Siendo parte de un problema que la creación del CSIRT y la cooperación con Bogotá mediante capacitaciones a empleados públicos podría mejorar.

C. Insuficiente vinculación internacional ligada a la temática. Si bien la Ciudad de Córdoba ha conformado el Hub de ciberseguridad para posicionarse, aún carece de vinculación internacional en relación a la temática. A pesar de que la Ciudad forma parte de alianzas como la *LatAm Smart Cities Alliance,* no ha estado participando en proyectos, actividades o cooperación alguna con actores internacionales en materia de ciberseguridad o ciberataques. Es por eso que el proyecto será importante para la creación de

nuevos vínculos y relaciones que sean beneficiosas para los actores involucrados.

Aceptar la existencia de vulnerabilidades y comprender la posibilidad de emergencia de amenazas latentes es un gran paso para emprender una planificación que permita hacerles frente a problemáticas locales. Esto es lo que busca el siguiente plan de implementación, el cual procura desarrollar una estrategia de internacionalización a través de la cooperación entre actores, enfocando los recursos y esfuerzos mutuos hacia el fortalecimiento de tal vinculación para la resolución a los problemas anteriormente mencionados.

Plan de Implementación

Objetivo General:

Fortalecer la cooperación internacional entre la Municipalidad de Córdoba y el Distrito de Bogotá para la creación de un Equipo de Respuesta ante Emergencias Informáticas (CSIRT) en la Ciudad de Córdoba.

Objetivos Específicos:

Con efecto de concretar dicho objetivo, se persiguen los siguientes *Objetivos Específicos:*

1. Consolidar las capacidades de los actores vinculados a la gestión de la política de ciberseguridad a través de la captación de recursos y cooperación nacional e internacional.

2. Fortalecer la protección de las infraestructuras críticas e infraestructuras de tecnología de la información (TI)

3. Fomentar la capacitación en competencias digitales en la población con hincapié en ciberseguridad, brindando programas de comunicación, concientización, formación técnica y educación.

Alcance:

Alcance temporal:

El alcance temporal de la propuesta se extiende para el Periodo 2023-2024, siendo de mediano plazo y con la posibilidad de la extensión de la propuesta, ya que el plan está basado en tecnologías y amenazas que se actualizan constantemente en una red que aún se está construyendo.

Alcance geográfico:

En términos geográficos el plan se adapta a la Ciudad de Córdoba, atendiendo a las necesidades que tiene la misma respecto a la seguridad de su población e instituciones. Se destaca a su vez la importancia de un plan de internacionalización en un contexto en el que la paradiplomacia toma cada vez mayor relevancia para posicionar y proteger a la ciudad mediante proyectos como este.

Alcance institucional:

Esta propuesta incluye de forma integral a la Secretaría de Planeamiento, Modernización y Relaciones Internacionales, con la cooperación del HUB de Ciberseguridad de la Ciudad de Córdoba y al Laboratorio de Innovación CorLab.

Recursos y presupuesto:

Recursos Humanos:

Correspondiente a la sección de recursos humanos, se debe contar con un director que se encargue de la administración y puesta en marcha del grupo de expertos, que supervise al equipo y a sus actividades, se encargue de la gestión presupuestal y la vinculación externa del CSIRT, ya sea con superiores, otros CSIRT, organizaciones, empresas o países.

Definido el director, este vincula y contrata al personal con las habilidades requeridas para las funciones a realizar en cada sector. Este centro de expertos tiene una composición tal

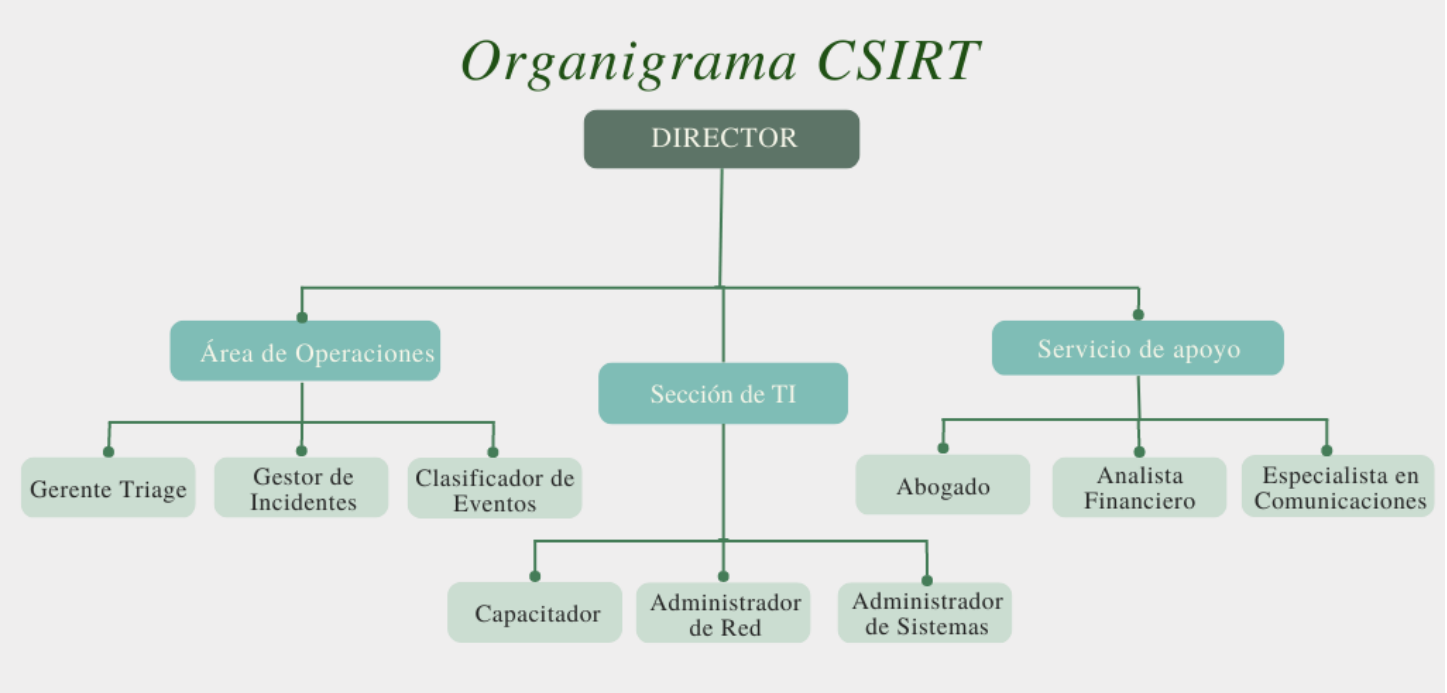
que independientemente de la posición que ocupe cada persona en la estructura, el personal debe tener conocimientos amplios en las demás áreas a fin de evitar fallas en el CSIRT.

Por debajo del director el equipo de expertos se divide en 3 áreas de igual calibre, cada una con un líder encargado de la representación y el mando de cada sector como también de la comunicación entre áreas y la dirección. Constituyéndose así:

- *Área de operaciones:* Compuesta por 1 líder y 3 especialistas en incidentes.
    1. Gerente Triage: Sus tareas se basan en clasificar y priorizar los eventos y asignar casos al personal técnico.
    2. Gestor de Incidentes: Analiza incidentes, monitoreo, registro y respuesta. Coordina la respuesta ante incidentes y colabora con el resto de áreas y personal para resolver un incidente.
    3. Clasificador de eventos: Provee la asistencia inicial de respuesta a incidentes y clasifica y prioriza la información recibida de un caso.
- *Sección de TI:* Compuesta por 1 líder y 3 especialistas técnicos.
    1. Capacitador: Se encarga de desarrollar material técnico. Desarrolla y publica documentos para el CSIRT. Informa y capacita a funcionarios y a los diversos actores que se involucren en el proyecto.
    2. Administrador de Red: Este puesto es el encargado de gestionar y mantener la infraestructura de red del CSIRT. Ayuda a su vez en la respuesta a incidentes en casos relacionados a redes.
    3. Administrador de Sistemas: Administra y mantiene los sistemas dentro del CSIRT. Asiste a la respuesta ante incidentes cuando se necesita a expertos en sistemas. Gestiona el acceso a datos e información crítica.
- *Servicio de apoyo*: Compuesta por 1 abogado, 1 analista financiero, 1 especialista en comunicaciones.
    1. Abogado: Brinda apoyo jurídico y la respuesta ante ataques cibernéticos en términos legales.
    2. Analista financiero: Administra el presupuesto y las finanzas del centro de expertos.
    3. Especialista en comunicaciones: Gestiona la prensa y se encarga de la comunicación y divulgación del material técnico para capacitar e informar a la población sobre el CSIRT y las amenazas cibernéticas.

Cuadro N° 3

Organigrama CSIRT Córdoba



Fuente: Elaboración propia.

Recursos financieros, no financieros, tecnológicos y materiales.

Cuadro N°2

Recursos financieros, no financieros, tecnológicos y materiales.

Recursos			
Financieros	**No financieros**	**Tecnológicos**	**Materiales**
Honorarios de 11 nuevos trabajadores	Conocimientos y especializaciones en Ciberseguridad y Tecnologías de la Información;	Desarrollo de estructuras de red seguras y compromiso de actualización y mantenimiento.	Computadoras
Gastos en viáticos por viajes destinados a la cooperación	Conocimientos en sector legal, económico y de la comunicación	Conexión a internet y impresoras	Guías y manuales
Infraestructura y espacios de reunión	Know-how	Bases de datos	Impresoras

	Vinculación local e internacional.		Celulares y teléfonos de emergencia
	Conocimientos y experiencia en internacionalización.		
	Voluntad de la Municipalidad de Córdoba y el Distrito de Bogotá		
	Capacitaciones internas brindadas al personal		

Fuente: Elaboración propia.

Los recursos financieros provienen del presupuesto anual de la Secretaría de Planeamiento, Modernización y Relaciones Internacionales de la MC, ya que este plan de implementación se lleva a cabo como una iniciativa de parte del Municipio.

Tal es así que se toman en cuenta en la elaboración del presupuesto a los recursos humanos contratados sin contar el costo de los recursos materiales, siendo considerados en el presupuesto anual del Municipio al ser preexistentes al desarrollo de este plan.

El presupuesto destinado para la Secretaría de Planeamiento, Modernización y Relaciones Internacionales en el año 2022 (Municipalidad de Córdoba, 2022), es de $470.633.180,87, el cual contempla gastos de infraestructura y mantenimiento necesarios para el desarrollo del plan de implementación.

En relación a los profesionales incorporados los cuales serán capacitados en el marco de la cooperación y el intercambio de información con el Distrito de Bogotá, se incorporan 11 trabajadores a la estructura municipal con un salario neto aproximado con una base de $240.512 por mes de acuerdo al sueldo de un funcionario de rango medio de la SPMRI publicado en el último informe del sitio web de la Municipalidad de Córdoba (Municipalidad de Córdoba, 2021). Siendo en total un presupuesto mensual de $1.545.632 en relación a la contratación de profesionales para llevar a cabo el proyecto.

Para establecer el grupo es necesario contar con 8 computadoras de alto rendimiento que rondan los $140.000. Resultando un total de $1.120.000.

En base al costo de los viáticos necesarios para la cooperación con Bogotá, siendo 1 taller colaborativo al inicio del proyecto y 6 mesas de diálogo anuales teniendo en cuenta también que 3 podrían realizarse con modalidad virtual, suman total 4 viajes a Colombia con

un presupuesto aproximado de $600.000 para la ejecución de la Alianza entre Córdoba y el Distrito de Bogotá.

En caso de alquilar nuevas oficinas, nos encontraríamos con un precio que se aproxima a los $960.000 anuales.

Sumando estos costos, y agregando un monto de 10% del total para gastos extras y emergencias, el presupuesto final anual para la creación y mantenimiento de un CSIRT en la Ciudad de Córdoba sería de $23.238.342 finales en el primer año del proyecto.

Al contar con un presupuesto anual de $470.633.180,87, el costo del plan de implementación resultaría de un 4,94% del porcentaje total del presupuesto municipal en la SPMRI.

Acciones específicas:

En la siguiente matriz general del plan de internacionalización se sintetizan el objetivo general, los objetivos específicos y sus correspondientes acciones específicas, las cuales indican cómo operar para llevar a cabo tales objetivos. También se determinan quiénes son los actores responsables de cada objetivo y sus acciones.

Cuadro N°4

Matriz de acciones del Plan de Implementación.

Objetivo General: Fortalecer la cooperación internacional entre la municipalidad de Córdoba y el distrito de Bogotá para la creación de un Equipo de Respuesta ante Emergencias Informáticas (CSIRT) en la Ciudad de Córdoba			
N°	Objetivos Específicos	Acciones	Actores Involucrados
1	Consolidar las capacidades de los actores vinculados a la gestión de la política de ciberseguridad a través de la captación de recursos y cooperación	1.1 Solicitar la cooperación a Bogotá y asegurar el compromiso de participación técnica y política para la ayuda mutua.	Intendente y Secretaría de Planeamiento, Modernización y Relaciones Internacionales, Distrito de Bogotá a través de la Alta Consejería TIC y el área de Relaciones Internacionales.
		1.2 Realizar un taller de trabajo colaborativo para examinar los	Secretaría de Planeamiento, Modernización y Relaciones

	nacional e internacional.	puntos comunes de Córdoba y Bogotá con el fin de elaborar una hoja de ruta para llevar a cabo la propuesta.	Internacionales, Distrito de Bogotá a través de la Alta Consejería TIC y el área de Relaciones Internacionales.
		1.3 Ejecutar al menos 3 mesas de diálogo durante cada semestre con Bogotá.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba, Distrito de Bogotá a través de la Alta Consejería TIC y el área de Relaciones Internacionales.
		1.4 Implementar la hoja de ruta creada por la Alianza, recibiendo y brindando apoyo técnico, y fomentando el intercambio de conocimientos y nuevas tecnologías.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba, Distrito de Bogotá a través de la Alta Consejería TIC y el área de Relaciones Internacionales.
		1.5 Realizar un foro de participación organizado por el HUB de Ciberseguridad para presentar el proyecto con la presencia de representantes de Bogotá y otros CSIRT, organizaciones e instituciones para fomentar la cooperación.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba, HUB de Ciberseguridad, Laboratorio de Innovación CorLab, Distrito de Bogotá a través de la Alta Consejería TIC y el área de Relaciones Internacionales.
2	Fortalecer la protección de las infraestructuras críticas e infraestructuras TI	2.1 Analizar el contexto para identificar infraestructuras críticas y actores fundamentales para desarrollar acciones conjuntas.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba, HUB de Ciberseguridad, Laboratorio de Innovación CorLab.
		2.2 Establecer y gestionar la infraestructura de red del CSIRT.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba.
		2.3 Establecer equipos sectoriales de operaciones, TI y servicio de apoyo ante incidentes cibernéticos.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba.
		2.4 Clasificar y priorizar eventos y asignar casos al personal	Secretaría de Planeamiento, Modernización y Relaciones

		especializado	Internacionales, CSIRT Córdoba.
		2.5 Co-crear una base de datos junto a Bogotá que contenga información y datos sobre posibles amenazas y su prevención.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba, Distrito de Bogotá a través de la Alta Consejería TIC y el área de Relaciones Internacionales.
3	Fomentar la capacitación en competencias digitales en la población con hincapié en ciberseguridad, brindando programas de comunicación, concientización, formación técnica y educación.	3.1 Emitir comunicados ante incidentes.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba.
		3.2 Co-crear una "Guía de buenas prácticas en Ciberseguridad" con Bogotá para divulgar en instituciones públicas y privadas incluyendo a la Municipalidad	Secretaría de Planeamiento, Modernización y Relaciones Internacionales, CSIRT Córdoba, Distrito de Bogotá a través de la Alta Consejería TIC y el área de Relaciones Internacionales.
		3.3 Crear programas de educación, formación técnica y concientización para el personal municipal y la población.	Secretaría de Planeamiento, Modernización y Relaciones Internacionales.

Fuente: Elaboración propia.

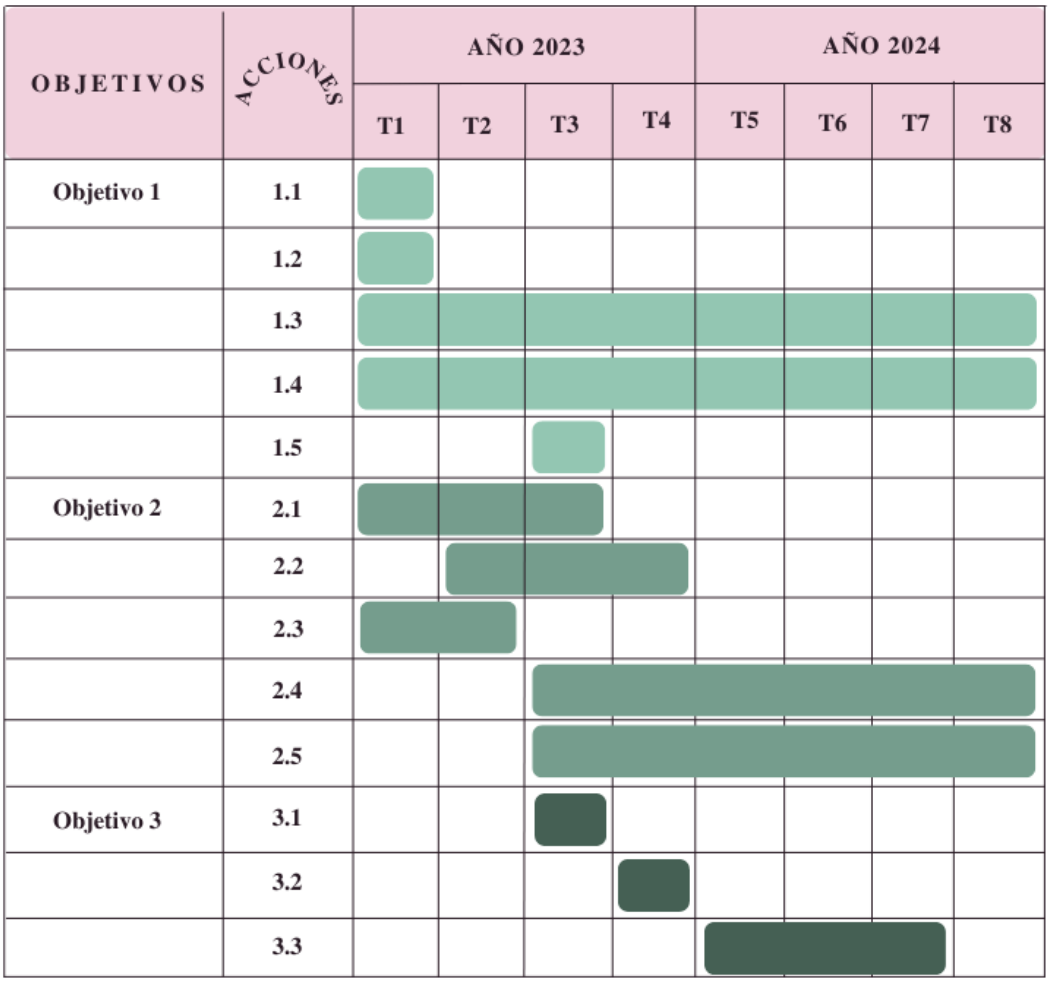
Marco de tiempo:

Se propone que el plan sea de mediano plazo y tenga un alcance temporal de dos años para el período 2023-2024, dividiendo sus actividades en ocho trimestres y con la posibilidad de extensión por el surgimiento de nuevas tecnologías y posibles amenazas que componen a la ciberseguridad y alcanzan al CSIRT.

A Continuación, se presenta un Diagrama de Gantt que refleja el tiempo estimado para la planificación y realización de las actividades.

Cuadro N°5

Distribución de acciones en marco de tiempo



Fuente: Elaboración propia.

Propuesta de evaluación:

En el siguiente cuadro, se presentan una serie de indicadores que permiten medir el éxito de los objetivos del plan y recolectar información que permite continuar de forma eficaz a través de la realización del mismo. Estos indicadores nos permiten observar si las acciones son exitosas, si están prosperando de forma correcta o si se acercan al fracaso.

Cuadro N°6

Propuesta de evaluación

Objetivos	Indicadores
Objetivo 1: Consolidar las capacidades de los actores vinculados a la gestión de la política de ciberseguridad a través de la captación de recursos y cooperación nacional e internacional.	1 taller de trabajo colaborativo con Bogotá. 3 mesas de diálogo por semestre. 1 hoja de ruta. 1 foro de participación. Cooperar con al menos 3 CSIRT durante el plan de implementación.
Objetivo 2: Fortalecer la protección de las infraestructuras críticas e infraestructuras TI	Disminución del porcentaje de la población víctima de ciberataques. 2 proyectos de colaboración conjunta. Aumento en el porcentaje de percepción de seguridad. Envío de 3 comunicados mensuales a Bogotá. Creación de una base de datos junto a Bogotá. Contacto con al menos 5 nuevos actores para formar nuevos tipos de cooperación. 6 reuniones anuales con los directores de infraestructuras críticas. Conformación de focus groups para medir las percepciones de seguridad cibernética. Medir porcentaje de la población que fue víctima de ciberataques. Porcentaje de la población que accede a compartir sus datos para mejorar la seguridad de la red.
Objetivo 3: Fomentar la capacitación en competencias digitales en la población con hincapié en ciberseguridad, brindando programas de comunicación, concientización, formación técnica y educación.	2 talleres de capacitación conjunta para el director y los líderes. 1 reunión mensual con personal de otras áreas de la municipalidad. Encuestas poblacionales sobre acceso a capacitaciones e información. Porcentaje de la población con acceso a medios digitales.

Fuente: elaboración propia.

Conclusión

A lo largo del trabajo, se indaga sobre la incorporación de nuevas tecnologías en la administración pública y el rol fundamental de la ciberseguridad en las Smart Cities, para establecer un lineamiento a seguir frente a las nuevas amenazas que ésta trae aparejadas.

La planificación estratégica del presente reporte permite a la Municipalidad de Córdoba estrechar relaciones con una ciudad cúspide en materia de ciberseguridad como lo es Bogotá y posibilita, a través de la creación del CSIRT, redefinir la estructura organizacional, al determinar un grupo especializado mediante la creación de nuevos roles y funciones además de establecer nuevas políticas públicas para superar las vulnerabilidades y amenazas cibernéticas que vienen de la mano con el desarrollo de nuevas tecnologías y las Smart Cities.

Debido al crecimiento de los ataques cibernéticos en gobiernos locales de todo el mundo, se debe entender a la Ciberseguridad como una problemática que atraviesa todo tipo de fronteras.

La internacionalización de la Municipalidad busca desarrollar una estrategia de Cooperación Internacional a través de alianzas y vínculos estratégicos con diversas ciudades, fomentando el desarrollo local.

Es por eso que se ha elaborado una propuesta que permite proteger de ataques cibernéticos a la población de la Ciudad de Córdoba a través de mejoras en materia de Ciberseguridad, área que detenta la falta de accionar del Municipio en la problemática.

A tal efecto, se han propuesto una serie objetivos y acciones, buscando consolidar una política de ciberseguridad, en marco de la colaboración con el Distrito de Bogotá y la cooperación con diversos actores nacionales e internacionales, fortaleciendo la protección de las infraestructuras críticas e infraestructuras de tecnología de la información (TI) de la ciudad y fomentando la capacitación en competencias digitales en el Municipio y la población en general, en un lapso temporal de mediano plazo (2 años).

Para la realización del presente trabajo se han destacado una serie de fortalezas, resaltando un alto nivel de institucionalización de las Relaciones Internacionales de la MC y un gran interés y voluntad política en la temática, ya que se cuenta con antecedentes como el HUB de Ciberseguridad y la cooperación intersectorial con el CorLab. Sumando a las nuevas oportunidades se señala la posibilidad de cooperar con una ciudad distinguida en la materia,

forjar lazos que propicien la generación de nuevos vínculos, mejorar las capacidades de defensa de la ciudad, limitar las pérdidas que causa la delincuencia cibernética y lograr posicionar a Córdoba como una de las pioneras a nivel Latinoamérica en la creación de un CSIRT propio para la Ciudad.

En contraposición se analizaron a su vez debilidades, destacando la falta de legislación en materia de ciberseguridad, la falta de sistematización de datos e información al ser un área relativamente nueva para la administración pública, el desconocimiento y la ausencia de capacitaciones en la temática, la falta de coordinación entre jurisdicciones y la escasa participación en el presupuesto municipal.

Teniendo en cuenta en el análisis la existencia de una serie de principales amenazas como la inestabilidad económica en la que se sumerge el país y la falta de coordinación entre nación y municipio, el lento desarrollo legislativo y el aumento de la utilización de nuevas tecnologías sin criterios de ciberseguridad.

Como resultado, el presente trabajo busca la profundización y el pleno desarrollo de la Ciberseguridad en la Municipalidad de Córdoba, a través de la cooperación internacional e interinstitucional, considerando que es un asunto que reviste vital importancia para el correcto funcionamiento de la Ciudad y sus entidades e instituciones, con la finalidad de proteger la seguridad, integridad y bienestar de la población y sus datos, al mejorar las relaciones intersectoriales en el municipio y enriqueciendo las relaciones internacionales con gobiernos no centrales a través del establecimiento de nuevos contactos formales e informales, en vista de posicionar a la ciudad de Córdoba en la materia.

Referencias

Alta Consejería Distrital TIC. (2021). Avances 2020: Bogotá Territorio Inteligente. https://tic.bogota.gov.co/documentos/avances-bogot%C3%A1-territorio-inteligente-2020

Ayllón Pino, B. (2009).Cooperación Sur – Sur: Innovación y Transformación en la Cooperación Internacional. Fund. Carolina: España.

BA-CSIRT. (s.f.). *Centro de ciberseguridad ciudadana*. Recuperado de:https://bacsirt.buenosaires.gob.ar/?u=home

Borghello, C & Temperini, M. (2013). *Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública*.Simposio Argentino de Informática y Derecho (SID),28 -43. http://sedici.unlp.edu.ar/handle/10915/94081

Carlini, A**.** (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *bie3: Boletín IEEE, (2)*,950-966.https://dialnet.unirioja.es/servlet/articulo?codigo=5998287

Carozo, E., Martínez, C., Vidal, L., Betarte, G., Blanco, A., Rodríguez, M., & Pérez, J. (2008). Análisis del desarrollo de un centro de respuesta nacional para la República Oriental del Uruguay. *Memoria Investigaciones En Ingeniería, (6)*,64-86.http://www.revistas.um.edu.uy/index.php/ingenieria/article/view/264

CERT -Bahia.(s.f).*Sobre O Cert Bahia*.Recuperado de: .https://certbahia.pop-ba.rnp.br/pages/about/

Ciberseguridad. (s.f.). *Ciberseguridad en Smart Cities*. Ciberseguridad.Recuperado de :https://ciberseguridad.com/guias/nuevas-tecnologias/smart-cities/amp/

Ciberseguridad. (2018). *Argentina: medidas de ciberseguridad*.Recuperado de: https://ciberseguridad.com/normativa/latinoamerica/argentina/#Medidas De Ciberseguridad

Cobo, C; Cortesi, S; Brossi, L; Doccetti, S; Lombana, A; Remolina, N; Winocur, R, y Zucchetti, A. (Eds.)**.** (2018). *Jóvenes, transformación digital y formas de inclusión en América Latina.* Montevideo, Uruguay: Penguin Random House.

Cornago, N. (1999). Diplomacy and paradiplomacy in the redefinition of international security: Dimensions of conflict and co‐operation.*Regional & Federal Studies, 9,(1), 40-57.https://doi.org/10.1080/13597569908421070*

Cornago,N. (2010).La descentralización como elemento de innovación diplomática: aproximación a sus causas estructurales y lógicas de acción en L.Maira.(Ed.), *La política internacional subnacional en América Latina,(pp.107-134)*.Libros del Zorzal: Buenos Aires.

CorLab. (s.f.). *Laboratorio de Innovación Govtech de la Municipalidad de Córdoba*.Recuperado de:.https://corlab.cordoba.gob.ar/

Cotino, L. & Sánchez, M. (2021). *Guía de ciberseguridad para ciudades inteligentes*.Banco Interamericano de Desarrollo. (M. Bouskela, G. Chona, A. Nowersztern, P. Zambrano-Barragán & I. Zapparoli, Eds.). http://dx.doi.org/10.18235/0003876

C4IR.CO. (2021, diciembre 16). Lineamientos para las ciudades a partir de los modelos de política de la Alianza Global G20 Ciudades Inteligentes. Recuperado de: https://c4ir.co/lineamientos-para-las-ciudades-a-partir-de-los-modelos-de-politica-de-la-alianza-global-g20-ciudades-inteligentes-2/

Gabinete de Transformación Digital de la República Dominicana. (2022). Agenda Digital 2030. República Dominicana.
.https://agendadigital.gob.do/documentos/#01JGWUNSVWZHSF4GTCV5F3H6B3N7VOZTVQ

Gabinete de Transformación Digital de la República Dominicana.(2022).Plan de Acción 2021-2024 de la Agenda Digital 2030. República Dominicana

.https://agendadigital.gob.do/documentos/#01JGWUNSVWZHSF4GTCV5F3H6B3N7VOZTVQ

G20 Global Smart Cities Alliance. (2020). Política Modelo: Política de rendición de cuentas de ciberseguridad. Política https://globalsmartcitiesalliance.org/?page_id=1690

Indela. (s.f.). *Indela Fund - Nosotros*. Recuperado de: http://indela.fund/nosotros/

Killcrece, G., Kossakowski, K., Ruefle, R. & Zajicek, M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRT´s). Pensilvania: Universidad Carnegie Mellon.

López Azumendi, S., Facchina, M., & Zapata, E. (2021). Liderazgo público y participación privada y de ciudadanos: la transformación digital de la ciudad de Córdoba en Argentina. *Policy Brief, #24*, 14. https://scioteca.caf.com/handle/123456789/1699?show=full

Municipalidad de Córdoba. (2019). *Córdoba una ciudad en cifras. Guía estadística de la ciudad de Córdoba*.https://prod-gobiernoabierto-media-20211201181351763900000001.s3.amazonaws.com/datos/Guia2019-version-final_bIwxG3z.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIA4F7OG6OIE3TCFZOG%2F20221023%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20221023T201859Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=b278348a9b6524429b830fa5fb34d835582de13de10f45df5549e81bdbfaa299

Municipalidad de Córdoba. (2019). *Organigrama*. Córdoba Gobierno. Recuperado de: https://cordoba.gob.ar/areas-de-gobierno/secretaria-de-planeamiento-modernizacion-y-relaciones-internacionales/organigrama/

Nicholas, P. (30 de enero de 2018). *Smart city resilience: Digitally empowering cities to survive, adapt, and thrive*. McKinsey. Recuperado de:https://www.mckinsey.com/business-functions/operations/our-insights/smart-city-resilience-digitally-empowering-cities-to-survive-adapt-and-thrive

Nieves, M. (2019). Uruguay y la ciberseguridad: entre los determinismos regionales y el proceso doméstico. *Selección de trabajos presentados en el IX Encuentro del CERPI y la VII Jornada del CENSUD*, 106-124. http://sedici.unlp.edu.ar/bitstream/handle/10915/116258/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Nye, J. (2010), "Cyber Power".Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power

Observatorio de Ciberseguridad en América Latina y el Caribe. (2020). *Observatorio de Ciberseguridad en América Latina y el Caribe*. Recuperado de: https://observatoriociberseguridad.org/#/about

Organización de los Estados Americanos (OEA). (s.f.). *Programa de Ciberseguridad.* OEA :CICTE: Ciberseguridad. Recuperado de: https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp

Programa Iberoamericano para el Fortalecimiento de la Cooperación Sur-Sur. (2011). Posición sobre la Cooperación Sur-Sur en el marco de la Cooperación Internacional para el Desarrollo de Diecinueve países Iberoamericanos. https://cooperacionsursur.org/biblioteca/#pifcss

Proyecto de Ordenanza N°9797 de 2021. [Concejo Deliberante de Córdoba]. Remitiendo el presupuesto general de gastos y cálculo de recursos - Ejercicio 2022. 22 de diciembre de 2022.

Resolución N°571 de 2021.[Municipalidad de Córdoba]. Escala Salarial de Mayo 2021. 28 de mayo de 2021.

Télam. (10 de Enero de 2017). La Ciudad de Buenos Aires tiene el primer centro de ciberseguridad en América Latina. *Télam digital*. Recuperado de: https://www.telam.com.ar/notas/201701/176186-caba-centro-ciberseguridad.htm

Van der Heide, M. (2020). *Estableciendo un CSIRT.* CSIRT CEDIA. https://csirt.cedia.edu.ec/proyectos-csirt/manual-estableciendo-un-csirt-de-thaicert-traducido-al-espanol/

Weisstaub, L & Kern, A. (2011). El debate sobre la cooperación sur-sur y su lugar en la política exterior de la Argentina. Revista Española De Desarrollo y Cooperacion, vol 27, 83-95.https://www.academia.edu/1853786/El_debate_sobre_la_cooperaci%C3%B3n_sur_sur_y_su_lugar_en_la_pol%C3%ADtica_exterior_de_la_Argentina?auto=citations&from=cover_page

Xalma, C. (2008). *Estudios SEGIB nº3:II Informe de la cooperación sur-sur en Iberoamérica. Secretaría General* Iberoamericana.https://www.segib.org/?document=ii-informe-de-la-cooperacion-sur-sur-en-iberoamerica-2008