ESTUDIO DEL SECTOR DE LA SOLICITUD PÚBLICA DE OFERTA CUYO OBJETO ES SELECCIÓN DE EMPRESAS COMERCIALIZADORAS DE BIENES Y SERVICIOS DE SOLUCIONES DE SEGURIDAD DIGITAL, SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD COMO ALIADOS PROVEEDORES PARA LA FIRMA DE ACUERDOS MARCO CON LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU.

1 INTRODUCCIÓN

De conformidad con los estatutos de la Empresa para la Seguridad y Soluciones Urbanas ESU, compilado mediante el Acuerdo número 102 del 8 marzo de 2021, y específicamente según el Artículo 6° Formas de Desarrollo del Objeto, la ESU definió, entre otras, la línea Estratégica de Tecnología, la cual consiste en "Soluciones tecnológicas, innovadoras y eficientes que contribuyen al mejoramiento de procesos de nuestros clientes". De igual forma, para poder ofrecer las líneas estratégicas definidas, en dicho artículo se determinó que la empresa desarrollará, entre otras, las siguientes actividades: a. Asesoría y consultoría; b. Comercialización y prestación de bienes y servicios; Gestión de proyectos (planeación, formulación, ejecución, evaluación e interventoría); Proveer redes y Servicios de Telecomunicaciones; e. Suministro y gestión de equipos, sistemas, redes e infraestructura tecnológica; f. Promover la investigación aplicada la innovación y la transferencia de conocimiento; g. Provisión de equipos, software y personal especializado en la identificación y prevención de ataques cibernéticos; h. Diseño, desarrollo, integración, licenciamiento y gestión de software y servicios informáticos; i. Diseño, construcción, gerencia y mantenimiento de obras públicas y privadas necesarias para el desarrollo de los proyectos de seguridad, logística, tecnología y/o sostenibilidad.

En tal sentido se hace oportuno y conveniente además de los estudios previos, llevar a cabo el estudio del sector para valorar el mercado desde diferentes perspectivas e identificar el sector al cual pertenece el servicio que se atenderá, como también el uso de la información para determinar las variables desde la óptica técnica, legal, financiera, logística, de riesgos, entre otras que soporte los requisitos a establecer en los pliegos de condiciones para surtir el proceso en referencia.

El desarrollo del presente documento se estará presentado en las siguientes etapas:

1. **Aspectos Generales:** Se encuentra conformado por el contexto económico, técnico y regulatorio.
2. **Análisis de la Oferta:** Se encuentra conformado por las empresas que pueden atender la necesidad así como la información correspondiente a la dinámica en la que opera el servicio.
3. **Análisis de la Demanda:** Información correspondiente sobre la prestación de bienes y servicios de Soluciones de Seguridad Digital, Seguridad de la Información y Ciberseguridad de la entidad para satisfacer las necesidades de sus clientes.

2 DEFINICIONES

AGN	Archivo General de la Nación
AI	Inteligencia Artificial
CONPES	Consejo Nacional de Política Económica y Social
CRC	Comisión de Regulación de Comunicaciones
DANE	Departamento Administrativo Nacional de Estadística
IPC	Índice de Precios al Consumidor
MIPYMES	Micro, pequeñas y medianas empresa
OCDE	Organización para la Cooperación y el Desarrollo Económicos
SGDAE	Sistema de Gestión Documental de Archivo Electrónico
TD	Transformación Digital
TIC	Tecnologías de la Información y las Comunicaciones
Seguridad Digital	Situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.
4RI	Cuarta Revolución Industrial

3 ASPECTOS GENERALES

Es un hecho relevante y de actualidad entender la transformación digital como aspecto fundamental para el crecimiento y competitividad de la economía colombiana, en los últimos años viene en crecimiento el desarrollo comercial de los negocios, más aún con los efectos de la pandemia ocurrida durante el año 2020 hasta la actualidad han mostrado la necesidad de fortalecer la digitalización. La revista semana en su edición 600 informa que el país ocupa el puesto 61 de 63 países que establece el ranking mundial de competitividad Digital, el segundo peor puesto de Latinoamérica, por lo que el gobierno nacional en la actualidad estableció la necesidad de invertir $121.619 millones en cinco años para crear las condiciones que permitieran a Colombia entrar con pie firme en la cuarta revolución industrial.

Es claro que la transformación digital va de la mano con los asuntos de conectividad, situación que en Colombia cerró el primer trimestre de 2020 con cifras positivas en dicha materia, según el último Boletín TIC. El país cuenta hoy con más de 7,1 millones de accesos fijos a Internet, 161 mil accesos más que los registrados al final de 2019.

El mismo informe muestra que todos los estratos socioeconómicos aumentaron su velocidad de descarga de Internet fijo en el último año. Por primera vez, desde que se registra el dato, todos los estratos socioeconómicos tuvieron, en promedio, una velocidad de descarga mayor a 10 Mbps, que les permite tener una experiencia más positiva del consumo de contenido en línea.

"Los datos expuestos en este boletín nos muestran que vamos por buen camino en nuestro objetivo de cerrar la brecha digital para tener un país más conectado, con mayor crecimiento económico y más equidad social, y que las políticas implementadas en los últimos 2 años por el gobierno del presidente Duque están dando resultados; debemos mantener este camino", dice la ministra, Karen Abudinen.

Trimestralmente, el Boletín de Tecnologías de la Información y las Comunicaciones (TIC) presenta los datos de los servicios de telecomunicaciones en Colombia. Entre estos se encuentran estadísticas de los servicios de Internet y telefonía, en sus segmentos tanto móvil como fijo.

En cuanto a conexiones móviles a Internet, el país cerró el primer trimestre con una cifra cercana a los 30 millones de accesos. De esta manera, se registran 6 accesos a Internet móvil por cada 10 colombianos. De éstos, 7 de cada 10 accesos móviles a Internet se realizan en tecnología 4G.

En cuanto a telefonía móvil, se registraron más de 66 millones de líneas en el país, de las cuales aproximadamente el 20% son en la modalidad pospago. La tasa de crecimiento de la modalidad pospago fue del 4,7 %, mientras que para prepago fue de 1,7%. Esto evidencia un aumento en la adquisición de planes de mayor consumo.

Para conocer con más detalles estos y otros datos de interés del sector TIC, invitamos a consultarlo en http://colombiatic.mintic.gov.co.[1]

Así mismo de acuerdo con los objetivos y estrategias presentados en el Plan Nacional de Desarrollo 2018-2022, el Gobierno Nacional tiene el plan de continuar con el fortalecimiento de las industrias 4.0. Como estrategias se fortalecerá las capacidades tecnológicas, de infraestructura, de capacitación de planes de promoción y divulgación que favorezca la apropiación e implementación tecnológica, con el fin de evolucionar hacia una transformación digital que permita una mayor eficiencia en la industria nacional. Así mismo, buscará articular iniciativas del sector privado a los SIES y la transformación empresarial para lograr la innovación y adopción de tecnología[2].

En Materia de Seguridad Digital, Seguridad de la Información y Ciberseguridad en Colombia, en el año 2011, se formuló el Documento CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa y en 2016 el Documento CONPES 3854 Política Nacional de Seguridad Digital, donde se buscó fortalecer y generar capacidades en el Gobierno Nacional para brindar seguridad y defensa tanto a los ciudadanos como a las instituciones en el Ciberespacio con un enfoque de gestión de riesgos y aunque se logró un avance en materia de seguridad digital, no se tuvo el mismo resultado en cuanto a confianza digital debido a que no se involucró de manera suficiente a las diferentes partes interesadas en la seguridad digital.

Luego, en el año 2018, se estableció la Política de Gobierno Digital mediante la expedición del Decreto 1008, en ella se indica que la seguridad de la información es uno de los elementos fundamentales para el desarrollo del Gobierno Digital y busca preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos en pro de la confianza digital. Para esto, el Ministerio de Tecnologías de Información y las Comunicaciones establece entre otras el Modelo de Seguridad y Privacidad de la Información (MSPI), alineado con las buenas prácticas de seguridad de la información (Norma ISO/IEC 27001:2013), con la Ley 1581 de 2012 de la Protección de Datos Personales y con la Ley 1712 de 2014 de Transparencia y del Derecho de Acceso a la Información Pública Nacional y que permite establecer el nivel de madurez de las entidades públicas en cuanto a seguridad digital. Este Ministerio también presentó el Plan TIC 2018-2022 El Futuro Digital es de Todos, con los proyectos e iniciativas del sector TIC, varios de estos relacionados con seguridad digital.

De manera adicional, en el año 2019, mediante la Ley 1955, se expidió el Plan Nacional de Desarrollo 2018 – 2022 Pacto por Colombia, Pacto por la Equidad que, en el Pacto/Línea VII. Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento, busca encaminar al país hacia una sociedad digital y del desarrollo de estrategias sobre seguridad digital en los territorios y en el Pacto/Línea I. Pacto por la legalidad: seguridad efectiva y

[1] https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/151386:Colombia-siguio-mejorando-las-cifras-de-conectividad-en-el-primer-trimestre-del-ano

[2] DNP: Plan Nacional de Desarrollo 2018 – 2020: Pacto por Colombia, pacto por la equidad.

justicia transparente para que todos vivamos con libertad y en democracia, se establece como estrategia para promover el control integral marítimo, terrestre, aéreo, fluvial, espacial y ciberespacial que el Gobierno nacional fortalezca las capacidades de ciberseguridad y ciberdefensa para garantizar los intereses nacionales.

Esta Ley, en el artículo 147 Transformación Digital Pública, establece la inclusión y actualización permanente de políticas de seguridad y confianza digital, así como, la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, como principios orientadores para los proyectos estratégicos de transformación digital.

Durante el mismo año, el Ministerio de Defensa Nacional formuló la Política de Defensa y Seguridad para la legalidad, el emprendimiento y la equidad de Colombia con el fin de promover la confianza digital. En el marco de esta política se establecen estrategias para fortalecer las capacidades militares de defensa en el ciberespacio y para liderar la lucha contra el delito transnacional, en áreas como la ciberseguridad y protección de infraestructura crítica.

También en 2019, se expidió el Documento CONPES 3795 Política Nacional para la Transformación Digital e Inteligencia Artificial, cuyo objetivo es aumentar la generación de valor social y económico a través de la transformación digital del sector público y del sector privado, para que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la 4RI. Dicha política, establece dentro de sus acciones, la formulación de una política pública sobre ciberseguridad para mejorar las capacidades del país al respecto.

En julio de 2020, en documento CONPES 3995, se formula una política nacional cuyo objetivo es establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de forma que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para esto, se plantearon los siguientes objetivos: 1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país, 2. Actualizar el marco de gobernanza para la seguridad digital de forma que se aumente su grado de desarrollo y 3. Analizar la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías para preparar al país para los desafíos de la 4RI.

3.1 Contexto Regulatorio

El propósito de la estrategia regulatoria es apalancar la transformación digital del Estado y el uso de tecnologías emergentes a través de la reinvención o modificación de los procesos, productos o servicios para asegurar la generación de valor en lo público.

El artículo 147 de la Ley 1955 del 2019 (Plan Nacional de Desarrollo) establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las

Comunicaciones (MinTIC). Así mismo, el CONPES 3975, que define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.

Teniendo presente el marco normativo y de política pública expuesto, se presenta a continuación el Marco de Transformación Digital para el Estado:

¿Por qué es importante la Transformación Digital para el Estado?

- La Transformación Digital (TD) en el Gobierno es un compromiso de las entidades públicas y la forma más eficaz de brindar mayor calidad de vida para las personas y mayor competitividad para las empresas en un contexto social, económico y cultural marcado por la Cuarta Revolución Industrial (4RI).

- La TD apalanca los propósitos de la Política de Gobierno Digital fomentando el desarrollo de iniciativas para generar beneficios a la ciudadanía y al Estado.

- En el Estado, la TD implica procesos de cambio con visión a largo plazo, en donde el uso de las tecnologías digitales involucra no sólo el aspecto tecnológico, sino también los procesos y la cultura de las entidades públicas.

- La TD busca mejorar la relación Estado-ciudadano mejorando el acceso a la información pública, la provisión de trámites y servicios más ágiles y efectivos para lograr una interacción más sencilla y más satisfactoria con las entidades públicas.

¿Qué plantea el Marco de Transformación Digital para el Estado?

El propósito del Marco es apalancar la transformación digital del Estado y el uso de tecnologías emergentes a través de la reinvención o modificación de los procesos, productos o servicios para asegurar la generación de valor en lo público.

A través de cinco pasos esenciales del Marco de Transformación Digital, las entidades podrán iniciar su transformación digital en la que se deben desarrollar las siguientes acciones estratégicas:

i) Conformar el equipo de transformación digital;

ii) Definir la visión digital y la hoja de ruta de la transformación digital;

iii) Evaluar el estado actual y eliminar barreras que impidan o ralenticen la transformación digital;

iv) Ejecutar la ruta e implementar proyectos de transformación digital;

v) Preparar y evaluar las acciones relacionadas con el inicio y puesta en marcha de soluciones de transformación digital.

El Marco también cuenta con un kit de herramientas que se pone a disposición de manera gratuita a todas las entidades públicas:

- **Herramienta de Transformación Digital:** facilita la priorización de procesos para la transformación digital de las entidades públicas. Con esta herramienta se busca, además, revisar los modelos de gestión y procesos actuales para identificar lo que se quiere mejorar; medir el grado de madurez digital de manera sencilla e identificar la brecha existente; identificar y priorizar proyectos de transformación digital; y gestionar la implantación de este tipo de proyectos.

- **Guía para el uso de tecnologías emergentes:** orienta en el uso y adopción de las nuevas herramientas digitales para crear servicios y procesos internos más eficientes, intuitivos y seguros.

- **Guía para el diseño de servicios digitales:** desarrolla lineamientos para transformar la experiencia de los ciudadanos a través de interacciones digitales centradas en ellos.

- **Guía para la automatización de procesos:** busca procesos ágiles a través de la automatización inteligente con capacidad de entregar flujos de trabajo 100% precisos.

¿Qué lograrán las entidades del Estado con la implementación del Marco de Transformación Digital?

Las entidades públicas contarán con un Plan de Transformación Digital que definirá su estrategia a seguir durante los siguientes dos años y en el que se plantearán las iniciativas y proyectos a desarrollar conforme con la priorización de áreas de la organización y procesos que se transformarán digitalmente.

La transformación digital permitirá desarrollar acciones para asegurar la gestión del cambio y asegurar la apropiación de las tecnologías emergentes.

El Modelo de Seguridad y Privacidad del Ministerio de las Tecnologías de Información y las comunicaciones fue actualizado mediante la Resolución 00500 de marzo de 2021 y donde se hace referencia las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI relacionadas con Seguridad Digital, Seguridad de la Información y Ciberseguridad:

- Constitución Política de Colombia. Artículos 15, 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.

- Ley 1712 de 2014. 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 103 de 2015. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública". Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.

3.2 Contexto Técnico

En concordancia con los esfuerzos realizados en Colombia por el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Programa Gobierno Digital, las entidades deben orientar esfuerzos para el aseguramiento de la infraestructura tecnológica crítica, el mantenimiento de ambientes seguros, el aseguramiento de sistemas y la definición de niveles mínimos suficientes para controlar los riesgos y amenazas de cualquier naturaleza. Así mismo, teniendo en cuenta que actualmente nos encontramos en un mundo globalizado, donde las comunicaciones y los servicios generalmente están soportados en plataformas tecnológica, y la automatización e integración de sistemas informáticos es indispensable de que el soporte técnico para estos sistemas y la garantía posventa es vital para asegurar la estabilidad de los servicios, la continuidad de las operaciones y hasta la existencia de cualquier empresa, institución o entidad.

En la actualidad, los ataques informáticos han evolucionado y se han automatizado, generando dos problemáticas principales: La primera requiere estar en la capacidad de brindar protección de forma independiente a cada una de las zonas de seguridad que ha definido para su operación (zona de

servidores, zona de usuarios, zona wifi, zona de administración, zona DMZ) y la segunda, brindar a cada zona un nivel de seguridad acorde a su nivel de criticidad, permitiendo contar con protección tanto contra amenazas conocidas como contra amenazas desconocidas. Si no se contara con esta protección se podría perder uno de sus activos más importantes que es la información, impidiendo cumplir las funciones administrativas y misionales, afectando directamente no sólo a otras entidades que interoperan con los sistemas de información.

De esta forma se apoya el modelo nacional de Ciberseguridad y Ciberdefensa liderado por el Gobierno Nacional desde 2011, establecido en el Conpes 3701, en el cual se fijaron los lineamientos de la política en ciberseguridad para desarrollar una estrategia nacional que contrarreste el incremento de amenazas informáticas que pudieran afectar significativamente al país. Así mismo, con el Conpes 3854 de 2016 se creó la política nacional de seguridad digital, que incorporó los componentes de gobernanza, educación, regulación, cooperación internacional y nacional, investigación y desarrollo, e innovación.

La ESU plantea su proyecto de Selección de Empresas de Bienes y Servicios de Soluciones de Seguridad Digital, Seguridad de la Información Y Ciberseguridad para su propia implementación y para generación de productos y servicios para sus clientes, planteando el siguiente camino estratégico de adopción y apropiación tecnológica, para lo cual requerirá de aliados tecnológicos estratégicos, que son el objetivo de estos estudios previos.

Los aliados estratégicos deberán estar en capacidad de ofrecer de manera conjunta cada una de los siguientes bienes y servicios.

Solución Gestión, Riesgo y Cumplimiento – GRC:

GRC es la colección integrada de capacidades que permiten a una organización lograr objetivos de manera confiable, abordar la incertidumbre y actuar con integridad[3].

GRC como acrónimo denota gobernanza, riesgo y cumplimiento, pero la historia completa de GRC es mucho más que esas tres palabras.

El acrónimo GRC fue inventado por la membresía de OCEG (originalmente llamado "Grupo de Ética y Cumplimiento Abierto") como una referencia abreviada a las capacidades críticas que deben trabajar juntas para lograr el Desempeño de Principios - las capacidades que integran la gobernanza, la gestión y la garantía del desempeño, riesgo y actividades de cumplimiento.

Si bien el acrónimo se utilizó ya en 2003, el primer artículo académico revisado por pares sobre el tema fue publicado en 2007 por el fundador de OCEG, Scott L. Mitchell, en el International Journal of Disclosure and Governance. Este documento innovador influyó en toda una industria de software y servicios.

Este fue el comienzo de los estándares GRC de código abierto.

3 https://www.oceg.org/about/what-is-grc/

Es importante recordar que las organizaciones se han gobernado y el riesgo y el cumplimiento se han gestionado durante mucho tiempo; de esta forma, GRC no es nada nuevo.

Sin embargo, muchos no habían abordado estas actividades de manera madura, ni estos esfuerzos se han apoyado entre sí para mejorar la confiabilidad del logro de los objetivos organizacionales.

En una organización con visión de futuro, GRC se considera una colección integrada de todas las capacidades necesarias para respaldar el principio de rendimiento.

GRC no es una carga para el negocio, lo respalda y lo mejora.

Las organizaciones deben abordar el desafiante clima empresarial actual. Incluso las pequeñas empresas, las organizaciones sin fines de lucro y las agencias gubernamentales enfrentan problemas que solo las grandes empresas tenían que enfrentar en el pasado. Ahora cuántos de estos factores tiene que lidiar:

- Las partes interesadas exigen un alto rendimiento junto con altos niveles de transparencia.
- Las regulaciones y la aplicación son siempre cambiantes e impredecibles.
- El crecimiento exponencial de las relaciones con terceros y el riesgo es un desafío de gestión.
- Los costos de abordar los riesgos y los requisitos se están saliendo de control.
- El impacto severo (y aterrador) cuando no se identifican las amenazas y oportunidades.

Consultoría especializada - Establecimiento de Sistemas de Gestión de Seguridad SGSI basado en la norma ISO27001:2013 y los lineamientos de Gobierno en Línea:

Un SGSI desde la visión desde el estándar internacional ISO/IEC 27001 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio (p.ej. en empresas públicas, organizaciones sin ánimo de lucro)[4].

El alcance de un SGSI puede incluir, en función de dónde se identifiquen y ubiquen los activos de información esenciales, total o sólo un parte de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.

El término seguridad de la información generalmente se basa en que la información se considera un activo que tiene un valor que requiere protección adecuada, por ejemplo, contra la pérdida de disponibilidad, confidencialidad e integridad.

Cada organización puede extender e integrar en un SGSI las tres características básicas iniciales de definición de la seguridad a otras adicionales como suelen ser la autenticidad, trazabilidad, no repudio, auditabilidad, según se considere oportuno para cumplir con los requerimientos internos y/o externos aplicables en cada actividad.

4 https://www.iso27000.es/sgsi.html

Consultoría especializada - Acompañamiento a la certificación ISO27001:2013:

La certificación ISO 27001[5], Sistemas de Gestión de seguridad de la información permite la gestión y control de los riesgos de la seguridad de la información en las organizaciones para las cuales la información y la tecnología son activos importantes de su negocio.

Mediante las mejores prácticas de seguridad de la información, las organizaciones que certifican su SGSI demuestran ante sus accionistas, clientes, autoridades, proveedores y demás partes interesadas, la debida diligencia en este importante aspecto y garantizan la aplicación adecuada de los recursos en las áreas de mayor impacto potencial, optimizando así sus inversiones y costos de seguridad.

Habilita y potencializa el uso de las más actuales herramientas de colaboración y de gestión de la información, protegiendo el valor de la confidencialidad, la integridad y la disponibilidad de la información para el negocio.

La implementación del sistema de gestión de seguridad de la información se constituye en una herramienta para la comunicación eficaz entre la alta dirección empresarial, los responsables de la gestión y custodia de la información y los clientes y demás interesados.

Previene y reduce eficazmente el nivel de riesgo, mediante la implantación de los controles adecuados; de este modo, prepara a la organización ante posibles emergencias y garantiza la continuidad del negocio.

Permite a la dirección monitorear, evaluar, asignar y gestionar los recursos necesarios para la seguridad de la información.

Incrementa el nivel de conciencia del personal respecto a los tópicos de seguridad de la información.

Consultoría especializada -Auditorías de Terceros:

Dentro de las definiciones del Modelo de Seguridad y Privacidad MPSI del Ministerio de las tecnologías de la Información y las comunicaciones, se define que las políticas deben tener un alcance que involucre los terceros de las entidades:

“La política establece la base respecto al comportamiento de personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la Entidad” [6]

Así mismo define en la fase 3 se realicen Evaluaciones de Desempeño mediante auditorías internas o externas, por esta razón se hace necesario realizar auditorías a todos los proveedores de Tecnología y soluciones de las entidades para poder determinar el nivel de riesgo presente y establecer controles que mitiguen dicho riesgo.

[5] https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion/
6 https://gobiernodigital.mintic.gov.co/692/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

Solución Centro de Operaciones de Seguridad SOC-NOC:

Un Centro de Operaciones de Seguridad (COS), (SOC en inglés) es una central de seguridad informática que previene, monitorea y controla la seguridad en las redes y en Internet. Los servicios que presta van desde el diagnóstico de vulnerabilidades hasta la recuperación de desastres, pasando por la respuesta a incidentes, neutralización de ataques, programas de prevención, administración de riesgos y alertas de antivirus informáticos.

Dotado de servidores, firewalls, sistemas de detección de intrusos, software antivirus y otros sistemas especializados, un COS monitorea la actividad en las redes e Internet en tiempo real, las 24 horas del día, los 7 días de la semana. Los datos eventos son analizados y rastreados por expertos certificados en estándares de seguridad.[7]

Servicios de Atención de Incidentes de Seguridad y Ciberseguridad:

Un equipo de respuesta a incidentes (también conocido como Equipo de respuesta a incidentes de seguridad informática) [CSIRT] es responsable de proporcionar servicios de respuesta a incidentes a parte o toda una organización. El equipo recibe información sobre posibles incidentes, los investiga y toma medidas para garantizar que se minimice el daño causado por las incidencias.[8]

La organización de una capacidad de respuesta a incidentes de seguridad informática (CSIRT) eficaz implica varias decisiones y acciones. Una de las primeras consideraciones debería ser crear una organización específica definición del término "incidente" para que el alcance del término sea claro. La organización debería decidir qué servicios debe proporcionar el equipo de respuesta a incidentes, considere qué estructuras y modelos del equipo pueden proporcionar esos servicios y seleccionar e implementar uno o más equipos de respuesta a incidentes. La creación de planes, políticas y procedimientos es una parte importante del establecimiento de un equipo, de modo que la respuesta a incidentes se realiza de forma eficaz, eficiente y coherente, de modo que el equipo esté capacitado para hacer lo que necesita para acabar.

El plan, las políticas y los procedimientos deben reflejar las interacciones del equipo con otros equipos. dentro de la organización, así como con partes externas, como las fuerzas del orden, los medios de comunicación y otras organizaciones de respuesta a incidentes. Esta sección proporciona no solo pautas que deberían ser útiles para organizaciones que están estableciendo capacidades de respuesta a incidentes, pero también asesoramiento sobre el mantenimiento y mejorar las capacidades existentes.

Solución Monitoreo de Productividad y Ciberseguridad de los usuarios:

El monitoreo de usuarios real es una tecnología de monitoreo pasivo que registra toda la interacción del usuario con un sitio web o un cliente que interactúa con un servidor o una aplicación basada en la nube. El seguimiento de la interacción real del usuario con un sitio web o una aplicación es importante

[7] https://es.wikipedia.org/wiki/Centro_de_operaciones_de_seguridad
8 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

para los operadores a fin de determinar si se atiende a los usuarios rápidamente y sin errores y, de no ser así, qué parte de un proceso empresarial está fallando. Software como servicio (SaaS) y proveedores de servicios de aplicaciones monitorean para administrar la calidad del servicio entregado a sus clientes. Los datos de monitoreo de usuarios reales se utilizan para determinar la calidad real del nivel de servicio entregada a los usuarios finales y para detectar errores o ralentizaciones en los sitios web. Los datos también pueden usarse para determinar si los cambios que se propagan a los sitios tienen el efecto deseado o causan errores.

Las organizaciones suelen monitorear sus usuarios para probar cambios dentro del entorno de producción o para anticipar cambios de comportamiento en un sitio web o aplicación mediante el uso de pruebas, monitorear la productividad y controlar la seguridad de los datos de la organizacion u otras técnicas. A medida que la tecnología se traslada cada vez más a entornos híbridos como la nube, los clientes pesados, los widgets y las aplicaciones, se vuelve cada vez más importante controlar el propio cliente.[9]

Solución Ciclo de Vida de desarrollo seguro – S-SDLC:

S-SDLC – Secure Software Development Life Cycle es un conjunto de principios de diseño y buenas prácticas a implantar en el SDLC, para detectar, prevenir y corregir los defectos de seguridad en el desarrollo y adquisición de aplicaciones, de forma que se obtenga software de confianza y robusto frente ataques maliciosos, que realice solo las funciones para las que fue diseñado, que esté libre de vulnerabilidades, ya sean intencionalmente diseñadas o accidentalmente insertadas durante su ciclo de vida y se asegure su integridad, disponibilidad y confidencialidad"[10]

Solución Análisis de Código Estático y Dinámico:

Las herramientas de análisis de código fuente, también conocidas como herramientas de prueba de seguridad de aplicaciones estáticas (SAST), están diseñadas para analizar el código fuente o versiones compiladas de código para ayudar a encontrar fallas de seguridad.[11]

Algunas herramientas están comenzando a incorporarse al IDE. Para los tipos de problemas que se pueden detectar durante la fase de desarrollo de software, esta es una fase poderosa dentro del ciclo de vida del desarrollo para emplear dichas herramientas, ya que proporciona retroalimentación inmediata al desarrollador sobre los problemas que podrían estar introduciendo en el código durante el código. desarrollo en sí. Esta retroalimentación inmediata es muy útil, especialmente cuando se compara con encontrar vulnerabilidades mucho más tarde en el ciclo de desarrollo.

Los escáneres de vulnerabilidades de aplicaciones web son herramientas automatizadas que escanean aplicaciones web, normalmente desde el exterior, para buscar vulnerabilidades de seguridad, como secuencias de comandos entre sitios, inyección SQL, inyección de comandos, recorrido de ruta y configuración de servidor insegura. Esta categoría de herramientas se conoce con frecuencia como herramientas de pruebas de seguridad de aplicaciones dinámicas (DAST). Hay disponible una gran

[9] https://es.wikipedia.org/wiki/Monitoreo_de_usuarios_reales
10 https://owasp.org/www-pdf-archive/OWASP-LATAMTour-Patagonia-2016-rvfigueroa.pdf
11 https://owasp.org/www-community/Source_Code_Analysis_Tools

cantidad de herramientas comerciales y de código abierto de este tipo y todas estas herramientas tienen sus propias fortalezas y debilidades.[12]

Solución Gestión continua de Vulnerabilidades:

El dominio de gestión de vulnerabilidades se centra en el proceso mediante el cual las organizaciones identifican, analizan y gestionan vulnerabilidades en el entorno operativo de un servicio crítico.

Cuando hablamos de vulnerabilidades, estamos discutiendo la característica o condición que, si es explotada por una amenaza (natural o creada por el hombre), hace que una entidad (es decir, una organización completa o cualquiera de sus partes constituyentes) sea susceptible a un riesgo. Cada aspecto del servicio se analiza en términos de los diversos activos que respaldan el servicio. Una vulnerabilidad en el servicio es el resultado de una vulnerabilidad en uno o más de sus activos. Los activos se dividen en categorías de personas, información, tecnología e instalaciones.

La gestión de vulnerabilidades es un componente clave en la planificación y determinación de la implementación adecuada de los controles y la gestión del riesgo. Es razonable decir que la gestión de vulnerabilidades es fundamental para la resiliencia cibernética

La explotación de una vulnerabilidad por una amenaza resulta en un riesgo para la organización. Ampliar la discusión de cuáles son las vulnerabilidades a cuán vulnerable es la organización a la interrupción o cuál es el impacto de explotar esta vulnerabilidad va más allá del dominio de la gestión de vulnerabilidades a una discusión sobre la gestión de riesgos. Es en la gestión de riesgos donde buscamos cuantificar el impacto de un peligro detectado.

Durante el proceso de gestión de vulnerabilidades, la organización a menudo puede descubrir vulnerabilidades que la llevan a desarrollar requisitos y criterios para los controles. Durante el proceso de gestión de controles, la organización desarrolla, implementa y mejora los controles que mitigan el efecto de un peligro.[13]

Hacking Ético:

El hacking ético es la práctica que consiste en utilizar las habilidades en sistemas informáticos y de red para ayudar a las organizaciones a probar sus mecanismos y procedimientos de seguridad con tal de identificar debilidades y/o vulnerabilidades.[14]

Las pruebas de un hacking ético se realizan con el conocimiento de los administradores y/o propietarios de los activos a probar, sin la intención de causar daños. Todos los hallazgos detectados se reportan para su subsanación.

[12] https://owasp.org/www-community/Vulnerability_Scanning_Tools
13 https://us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf
14 https://www.unir.net/ingenieria/revista/hacking-etico/

Servicios de Resolución de Vulnerabilidades:

Dentro del proceso de gestión de vulnerabilidades se encuentra la etapa de resolución, cuyo objetivo es reducir las vulnerabilidades más críticas presentes en las plataformas de TI y brindar a las entidades una ruta para la remediación de las vulnerabilidades como resultado de un análisis de los resultados de los escaneos de vulnerabilidades, de forma que se tenga en cuenta la criticidad de las vulnerabilidades y la sensibilidad de los activos afectados.

Este servicio entrega un plan de trabajo de las soluciones a las vulnerabilidades presentadas en la plataforma con priorización de implementación y lleva un registro de la gestión realizada y un reporte de indicadores de gestión.

Monitoreo de Marca Empresarial:

La marca empresarial se puede definir como un conjunto de información sobre una organización expuesta en internet (datos, imágenes, registros, noticias, comentarios, etc.), que genera su descripción en un entorno digital; es por esto, que la marca es de vital importancia tanto para la organización, como para sus colaboradores y sus grupos de interés.

Con el avance de las nuevas tecnologías, la web y las redes sociales (Twitter, Facebook, LinkedIn, etc.) hacen parte de los canales de comunicación de las organizaciones y se han convertido en herramientas de suma importancia para tener una retroalimentación en tiempo real de sus clientes y de sus usuarios, de ahí lo relevante para estar vigentes en estos medios de comunicación y ostentar de una buena reputación, teniendo en cuenta que esta es la que indica cuál es la percepción y valoración de los usuarios frente a la organización.

De manera adicional, existe el uso y mal uso de las bondades que ofrece internet, es por esto que las organizaciones deben investigar, monitorear y gestionar lo que sucede con sus marcas en la web, realizando un registro de las opiniones que dejan los usuarios y los medios sobre la compañía en redes sociales, foros, blogs, etc., también identificando las fortalezas de la compañía a través de las opiniones positivas y los aspectos a mejorar mediante las opiniones negativas y la información que pueda estar filtrada en la DarkWeb y DeepWeb.

Ejercicios de RedTeam:

Los ejercicios de ReadTeam o de seguridad ofensiva simulan ataques sobre la plataforma de TI de una organización, usando herramientas y técnicas usadas por los atacantes. Para esto se surte un proceso de emulación de escenarios de amenazas a los que se puede enfrentar una organización, donde se analiza la seguridad de la plataforma objetivo desde el punto de vista del atacante[15].

El objetivo de estos ejercicios es obtener una mejor comprensión de los problemas de seguridad a mitigar, la información sensible que se encuentra expuesta y los patrones potencialmente comprometedores que son accesibles desde el exterior de la organización.

[15] https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

Pruebas de Ingeniería Social:

Las pruebas de ingeniería social evalúan el comportamiento humano ante ataques diseñados para obtener información confidencial a través de la manipulación de usuarios de la organización. El objetivo de las pruebas es identificar los puntos fuertes y débiles de la organización en cuanto a la protección de la información que los funcionarios ejercen.

Estas pruebas están basadas en técnicas de interacción con los usuarios desde diferentes frentes, como llamadas telefónicas, visitas a las instalaciones, envío de correos, entre otros[16].

Pruebas de Intrusión Física:

Teniendo en cuenta que, en las instalaciones de las organizaciones es donde se encuentran los activos de información, las pruebas de intrusión física buscan identificar las fortalezas y debilidades de las organizaciones en cuanto a sus controles de seguridad física, los cuales protegen los activos de información organizacionales.

Solución Protección de Integral de Correo Electrónico:

Esta solución permite prevenir la entrega de correos no deseados ya que los detecta y elimina por medio de un análisis automático de todos los correos electrónicos entrantes enviados a un buzón de correo. Los análisis identifican las direcciones de correo electrónico y las direcciones IP que se sabe que son los remitentes de correos no deseados como spam o malware, así como las características que son típicas del spam, como la estructura y el contenido del correo.

Su objetivo es lograr un alto porcentaje de filtrado de correo no deseado para evitar recibir correos con contenido malicioso que faciliten la ejecución de ataques más avanzados.

Solución Control de Acceso a la Red:

Esta solución permite regular el acceso a la red organizacional con el fin de: mitigar ataques de día cero ya que permite prevenir la conexión a la red de equipos finales sin controles de seguridad, reforzar las políticas de control de acceso y administrar el acceso e identidad en la red, ya que se basa en las identidades de los usuarios finales autenticados[17].

Solución Protección de Integral de Estaciones de Trabajo:

Para la protección integral de las estaciones de trabajo se cuenta con soluciones como las herramientas EDR (End Detection and Response) que combaten las amenazas avanzadas y responde ante los incidentes presentados en los puntos finales de la red por medio del análisis de comportamiento, bloqueo de comportamiento, control de aplicaciones y listas blancas de aplicaciones y monitoreo de la red. De manera adicional, proporcionan detalles forenses que apoyan la respuesta a incidentes y

[16] https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)
[17] https://es.wikipedia.org/wiki/Control_de_acceso_a_red

facilitan la visibilidad de los comportamientos y procesos en el punto final y la administración de los activos físicos y de información.

De manera adicional, están los programas antivirus, cuyo objetivo es detectar y eliminar el software malicioso (virus, spyware, gusanos, troyanos, rootkits, pseudovirus, entre otros.). Existen varios mecanismos detección usados por los programas antivirus, entre ellos se encuentran los antivirus por firmas, los de detección heurística, los de detección por comportamiento y los de detección por sandbox).

Solución Control de Navegación – Proxy:

La solución de Control de Navegación permite restringir la navegación en internet de un usuario, de forma que se restrinja el acceso a sitios no deseados o se permita el acceso sólo a los sitios permitidos, de acuerdo con la necesidad de la organización. Esta solución es utilizada también para prevenir malware en la red organizacional.

Solución Firewalls y NGFW:

La solución firewall filtra las conexiones entrantes y salientes de una red, ofreciendo un nivel de seguridad a la red y hace que los dispositivos organizacionales establezcan únicamente las conexiones permitidas y evita ciberataques procedentes de internet sobre dichos activos. Estos dispositivos pueden ser un elemento de software o un dispositivo de hardware específico.[18]

Los NGFW o Next Generation Firewall incorporan funcionalidades adicionales de seguridad como antimalware, IPS (Sistema de Prevención Intrusiones), VPN, entre otros. Esta solución permite detectar y minimizar los riesgos activos, problemas de seguridad, actividades sospechosas, entre otros.

Solución Sandbox de Ciberseguridad:

La solución Sandbox de ciberseguridad proporciona un entorno aislado y dedicado para analizar y tomar acciones sobre amenazas que no han sido identificadas por las medidas convencionales de seguridad que usan firmas, como por ejemplo ransomware o amenazas avanzadas.

Solución Herramientas de Identificación y control de Amenazas Persistentes Avanzadas – APTs:

Esta solución identifica archivos y tráfico sospechoso de red, ejecuta archivos de entornos de sandbox, analiza el comportamiento y trata de identificar anomalías que indiquen la presencia de malware o un intento de explotación como parte de un APT (Amenaza Persistente Avanzada) que no son identificados por soluciones antivirus tradicionales ya que estas amenazas se caracterizan por permanecer indetectables el mayor tiempo posible utilizando técnicas de codificación evasivas para superar las barreras de seguridad tradicionales y robar datos sensibles.

[18] https://www.incibe.es/protege-tu-empresa/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

3.3 Contexto Económico

Desde el año 2009 la CRC ha tenido como una de sus funciones la de definir los "… criterios de eficiencia del sector y la medición de los indicadores sectoriales para avanzar en la sociedad de la información." A su vez, las bases del Plan Nacional de Desarrollo de 2014-2018 definieron que "[e]n línea con las mejores prácticas internacionales, la CRC publicará un informe anual sobre el efecto de la economía global de internet en la economía colombiana. Dicho informe incluirá recomendaciones de reglamentación a las entidades sectoriales correspondientes, que permitan preparar a los respectivos sectores para adaptación a la nueva economía de internet." Con base en los elementos citados y considerando que las redes de telecomunicaciones soportan el desarrollo de las aplicaciones en internet, la CRC desarrolló los estudios para definir la metodología de medición para la Economía Digital en Colombia, una situación directamente proporcional a los asuntos de seguridad Digital.

Según la Organización para la Cooperación y el Desarrollo Económicos –OCDE–, la economía digital se define como el resultado de un proceso de transformación desencadenado por las Tecnologías de la Información y las Comunicaciones (TIC). Su revolución ha abaratado y potenciado las tecnologías, al tiempo que las ha estandarizado ampliamente, mejorando así los procesos comerciales e impulsando la innovación en todos los sectores de la economía (OCDE, 2015).

Internet y la digitalización están cambiando la forma en que las personas, las empresas y los gobiernos interactúan. El acceso a banda ancha, la generación de confianza (protección al consumidor, protección de datos personales, seguridad digital), la apertura de mercados (mercado único digital, acuerdos comerciales), la generación de talento y de habilidades TIC, la apropiación tecnológica, el fomento al emprendimiento digital, la masificación del comercio electrónico y de medios de pago, entre otros, son elementos que impulsan la consolidación de una economía digital.

Y es que la economía digital no es tan solo una tendencia; empresas que han surgido en sectores como el transporte (Uber), audiovisual (Netflix), hotelero (AirbNb), comercio (Amazon) y muchas otras, demuestran cómo la tecnología puede cambiar industrias enteras. La digitalización y su impacto es tal, que ya se habla de una cuarta revolución industrial, este concepto se utiliza desde el 2006 en Alemania y recientemente fue objeto de análisis en el Foro Económico Mundial (WEF por sus siglas en inglés) de Davos. Es una revolución que utiliza la tecnología en todos los procesos productivos, transformando las economías radicalmente.[19]

[19] Medición de la Economía Digital en Colombia.pdf

Adopción de TIC. Puesto entre 141 países.
Fuente: WEF (2019).

Datos relevantes:[20]

- Aunque el acceso a internet de banda ancha ha crecido de manera importante en la última década, Colombia sigue rezagada frente a países de la región ocupando la posición 13 entre 17 países de América Latina en suscripciones a internet móvil.
- Colombia viene perdiendo posiciones de manera continua en el Índice de Gobierno Electrónico desde 2010.
- En 2018 ocupó la posición 61 entre 193 países.
- El bajo uso de cuentas en el sistema financiero y la confiabilidad del sistema postal limitan el desarrollo del comercio electrónico en el país.
- En el componente correspondiente a conocimiento del Índice de Competitividad Digital, Colombia ocupa la posición 57 entre 63 países.

[20] CPC_INC_2019-2020_Economia_digital.pdf - https://compite.com.co/wp-content/uploads/2019/11/CPC_INC_2019-2020_Economia_digital.pdf

- Solo el 35 % de los trámites en el país se puede empezar en línea. En Brasil esta cifra es de 75,4 %; en México, de 88,8 %, y en Uruguay aplica para el 100 % de los trámites.
- La adopción de tecnologías avanzadas es baja: solo el 8 % de las empresas utiliza internet de las cosas, el 3 % realiza impresión 3D y el 1 % usa robótica en sus procesos.
- Los estudiantes en Colombia obtienen el menor puntaje entre los países evaluados en el componente de lectura digital de las pruebas PISA.
- La velocidad de conexión a internet en Colombia no supera el promedio de América Latina y es una tercera parte del promedio OCDE.

Análisis macroeconómico

Teniendo en cuenta, que el presente proceso hace parte del sector servicios, tal como se indicó anteriormente, tenemos que el comportamiento económico ha sido el siguiente:

PIB

¿Qué es el PIB?

Es el total de bienes y servicios producidos en un país durante un período de tiempo determinado. Incluye la producción generada por nacionales residentes en el país y por extranjeros residentes en el país, y excluye la producción de nacionales residentes en el exterior.

PIB = Consumo + Inversión + Gasto del Gobierno + (Exportaciones – Importaciones)

Comportamiento del sector en el contexto local y nacional:

Información I trimestre 2021

En el primer trimestre de 2021pr, el Producto Interno Bruto, en su serie original, crece 1,1% respecto al mismo periodo de 2020pr. Las actividades económicas que más contribuyen a la dinámica del valor agregado son:

• Industrias manufactureras crece 7,0% (contribuye 0,9 puntos porcentuales a la variación anual).

• Administración pública y defensa; planes de seguridad social de afiliación obligatoria; Educación; Actividades de atención de la salud humana y de servicios sociales crece 3,5% (contribuye 0,5 puntos porcentuales a la variación anual).

• Agricultura, ganadería, caza, silvicultura y pesca crece 3,3% (contribuye 0,3 puntos porcentuales a la variación anual).

Tabla 1. Valor agregado por actividad económica
Tasas de crecimiento en volumen[1]
2021pr– Primer trimestre

Actividad económica	Tasas de crecimiento	
	Serie original	Serie corregida de efecto estacional y calendario
	Anual	Trimestral
	2021pr- I / 2020pr-I	2021pr - I / 2020pr - IV
Agricultura, ganadería, caza, silvicultura y pesca	3,3	1,8
Explotación de minas y canteras	-15,0	6,8
Industrias manufactureras	7,0	3,3
Suministro de electricidad, gas, vapor y aire acondicionado[2]	-1,3	0,7
Construcción	-6,0	17,0
Comercio al por mayor y al por menor[3]	-0,8	5,5
Información y comunicaciones	2,6	4,9
Actividades financieras y de seguros	4,9	1,1
Actividades inmobiliarias	1,7	0,6
Actividades profesionales, científicas y técnicas[4]	1,5	3,4
Administración pública, defensa, educación y salud[5]	3,5	-0,9
Actividades artísticas, de entretenimiento y recreación y otras actividades de servicios[6]	7,6	11,1
Valor agregado bruto	**1,0**	**3,3**
Total impuestos menos subvenciones sobre los productos	1,6	1,4
Producto Interno Bruto	**1,1**	**2,9**

Fuente: DANE, Cuentas nacionales

Información y comunicaciones: En el primer trimestre de 2021pr, el valor agregado de información y comunicaciones crece 2,6% en su serie original, respecto al mismo periodo de 2020pr:

Tasas de crecimiento en volumen[1]
2021pr– Primer trimestre

Actividad económica	Tasas de crecimiento	
	Serie original	Serie corregida de efecto estacional y calendario
	Anual	Trimestral
	2021pr -I/ 2020p -I	2021pr - I / 2020pr - IV
Información y comunicaciones	**2,6**	**4,9**

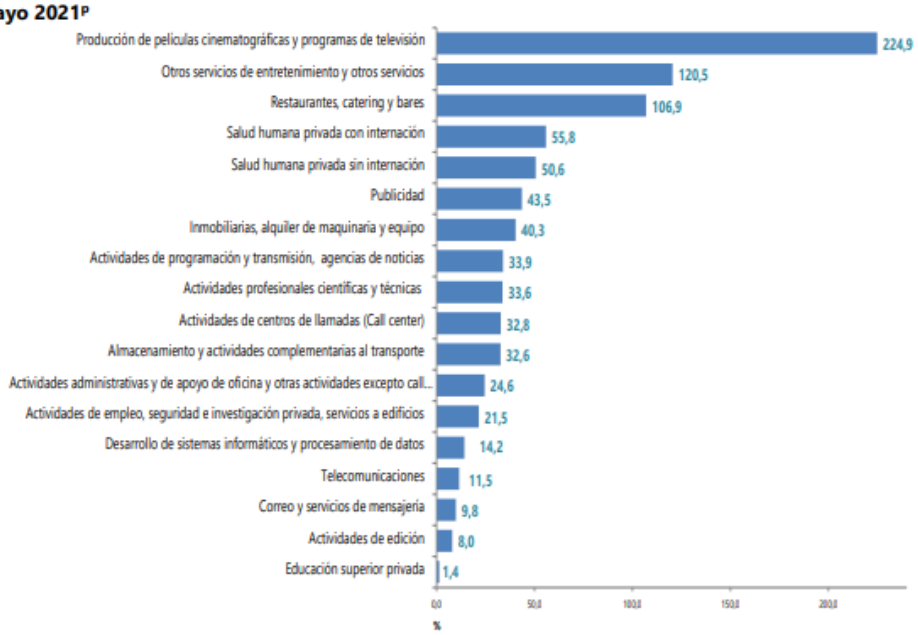
Fuente: DANE, Cuentas nacionales

En mayo de 2021, todos los subsectores de servicios presentaron variación positiva en los ingresos totales, en comparación con mayo de 2020.

Encuesta Mensual de Servicios (EMS)

Mayo de 2021

Gráfico 1. Variación anual de los ingresos nominales, según subsector de servicios
Total Nacional
Mayo 2021P



Fuente: DANE – EMS

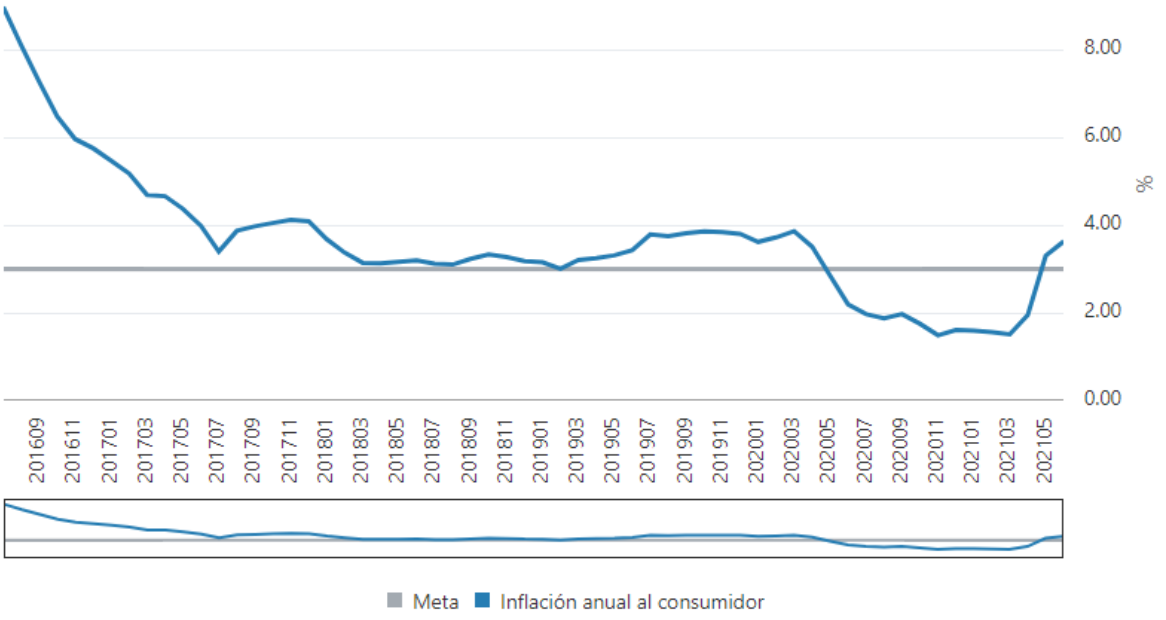
COMPORTAMIENTO GENERAL DE LAS IMPORTACIONES

De acuerdo con las declaraciones de importación registradas ante la DIAN en abril de 2021, las importaciones fueron US$4.696,7 millones CIF y presentaron un aumento de 51,7% con relación al mismo mes de 2020. Este comportamiento obedeció principalmente al aumento de 64,2% en el grupo de Manufacturas.

En abril de 2021, las importaciones de Manufacturas participaron con 76,9% del valor CIF total de las importaciones, seguido por productos Agropecuarios, alimentos y bebidas con 14,9%, Combustibles y productos de las industrias extractivas con 8,1% y otros sectores 0,1%

IPC:

El índice de precios al consumidor (IPC) mide la evolución del costo promedio de una canasta de bienes y servicios representativa del consumo final de los hogares, expresado en relación con un período base.



Fuente: Departamento Administrativo Nacional de Estadística (DANE)

TRM:

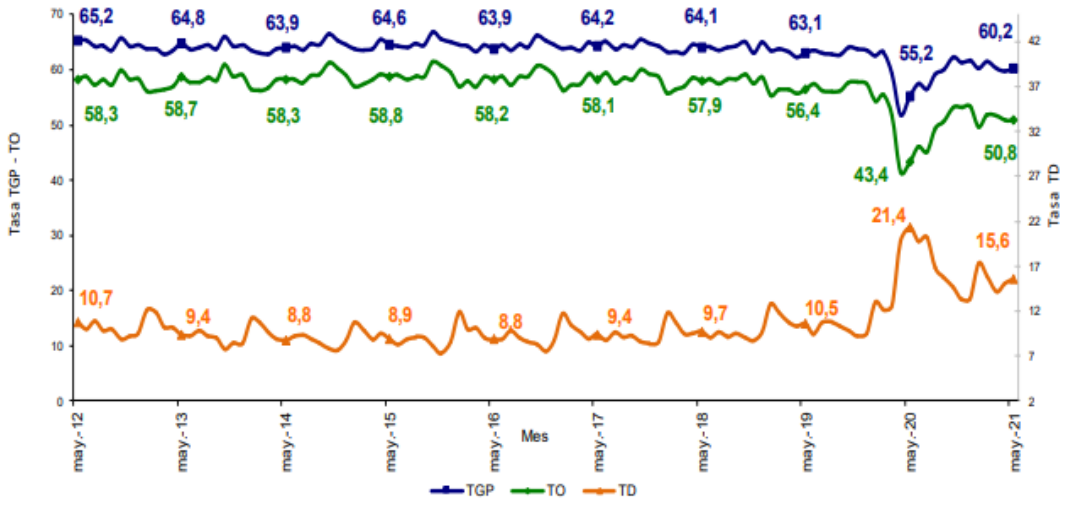
La tasa de cambio representativa del mercado (TRM) es la cantidad de pesos colombianos por un dólar de los Estados Unidos. La TRM se calcula con base en las operaciones de compra y venta de divisas entre intermediarios financieros que transan en el mercado cambiario colombiano, con cumplimiento el mismo día cuando se realiza la negociación de las divisas.

La TRM, se ha comportado de manera estable durante el ultimo año.

EMPLEO Y DESEMPLEO:

Para el mes de mayo de 2021, la tasa de desempleo fue 15,6%, lo que representó una reducción de 5,8 puntos porcentuales comparado con el mismo mes del 2020 (21,4%). La tasa global de participación se ubicó en 60,2%, lo que significó un aumento de 5,0 puntos porcentuales respecto al mismo periodo del 2020 (55,2%). Finalmente, la tasa de ocupación se ubicó en 50,8%, lo que representó un aumento de 7,4 puntos porcentuales comparado con mayo de 2020 (43,4%).

Gráfico 2. Tasa global de participación, ocupación y desempleo
Total nacional
Mayo (2012– 2021)



Fuente: DANE, GEIH.

En el período de estudio, el número de personas ocupadas en el total nacional fue 20.467 miles de personas. Las ramas que más aportaron positivamente a la variación de la población ocupada fueron Comercio y reparación de vehículos; Construcción; e Industria manufacturera con 4,1, 2,6 y 2,3 puntos porcentuales, respectivamente.

Rama de actividad	Total Nacional				
	Mayo 2021	Mayo 2020	Distribución %	Variación absoluta	Contribución en p.p.
Población ocupada	20.467	17.262	100,0	3.205	
Comercio y reparación de vehículos	4.061	3.349	19,8	713	**4,1**
Construcción	1.455	1.006	7,1	448	**2,6**
Industria manufacturera	2.148	1.752	10,5	396	**2,3**
Actividades artísticas, entretenimiento recreación y otras actividades de servicios	1.720	1.375	8,4	345	**2,0**
Administración pública y defensa, educación y atención de la salud humana	2.304	2.014	11,3	291	**1,7**
Transporte y almacenamiento	1.585	1.356	7,7	229	**1,3**
Alojamiento y servicios de comida	1.366	1.169	6,7	197	**1,1**
Agricultura, ganadería, caza, silvicultura y pesca	2.865	2.684	14,0	182	**1,1**
Suministro de electricidad, gas, agua y gestión de desechos^^	761	636	3,7	126	**0,7**
Actividades inmobiliarias	289	165	1,4	124	**0,7**
Actividades financieras y de seguros	369	282	1,8	87	**0,5**
Información y comunicaciones	301	250	1,5	51	**0,3**
Actividades profesionales, científicas, técnicas y servicios administrativos	1.242	1.217	6,1	26	**0,1**

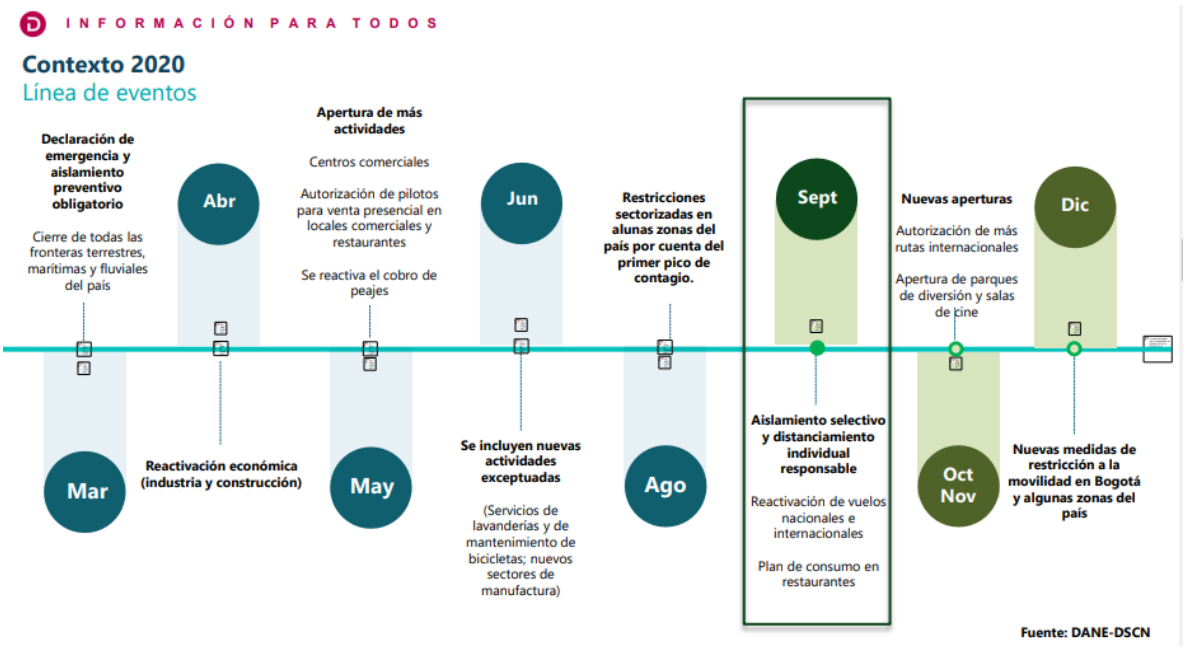
Fuente: DANE, GEIH.

Poco a poco la ocupación de las personas va incrementando y por medio de la presente contratación se espera aportar y contribuir a esa tasa de ocupación.

En primer lugar, es necesario partir de los datos como habilitadores de la implementación de tecnologías emergentes. Por lo tanto, surge la necesidad de digitalizar las interacciones de actores del gobierno y de la ciudadanía en general, con el objetivo de contar con información acerca de los retos y problemáticas de ciudad. Por lo tanto, el presente objetivo es buscar contribuir con insumos para que Medellín se convierta efectivamente en una ciudad movida por las tecnologías.

Según el Dane[21], en Colombia, la crisis del COVID-19 llegó en medio de la existente inestabilidad sociopolítica, tras las protestas masivas contra el gobierno, sumándose a las perspectivas económicas las cuales de por sí no eran buenas —producto de la bajada en los precios del petróleo y la desaceleración económica regional. Desde el año 2000 la economía en Colombia había crecido ininterrumpidamente, y durante los últimos diez años la pobreza se había reducido a la mitad. Sin embargo, el crecimiento económico del país se ha visto afectado por factores limitantes como el flujo acelerado y masivo de migrantes provenientes del vecino país de Venezuela y en la actualidad por el COVID-19. En la siguiente grafica el DANE detalla la línea de eventos de los sucesos del año 2020:

[21] https://www.dane.gov.co/files/investigaciones/boletines/pib/presen_rueda_de_prensa_PIB_IVtrim20.pdf



Fuente: https://www.dane.gov.co/files/investigaciones/boletines/pib/presen_rueda_de_prensa_PIB_IVtrim20.pdf

Según lo expresa en Banco Mundial en su página web, en Colombia las exportaciones están altamente concentradas en materias primas no renovables (petróleo en particular), lo que aumenta la exposición de la economía a los choques de precios. Además, Colombia es uno de los países de América Latina con mayor desigualdad en ingresos e informalidad del mercado laboral. Dice el reporte del Banco Mundial en su panorama general de fecha octubre 9 de 2020: "Después de desacelerarse al 1,4% en 2017, el crecimiento económico se incrementó hasta 3,3% en 2019, impulsado por un sólido consumo privado y una mayor inversión. El crecimiento estaba en camino a acelerarse aún más en 2020, pero la pandemia de COVID- 19 golpeó significativamente la economía y provocó una recesión muy profunda. El Gobierno respondió rápidamente a la crisis y tomó medidas decididas para proteger vidas y medios de subsistencia, y para apoyar la economía. En el frente fiscal, el Gobierno anunció un importante paquete fiscal para 2020 por un total de más de COP 31 billones (o casi el 3% del PIB de 2019), con el cual se proporcionaron recursos adicionales para el sistema de salud, se incrementaron las transferencias para los grupos vulnerables a través de la expansión de los programas existentes y el establecimiento de nuevos programas (Ingreso solidario, un programa de transferencias monetarias no condicionadas, y devolución de IVA para segmentos de la población de bajos ingresos), se retrasó el recaudo de impuestos en sectores seleccionados, se redujeron aranceles para las importaciones estratégicas en salud y se ayudaron a las empresas más afectadas a pagar la nómina de los empleados. El gobierno también estableció líneas especiales de crédito y garantías de préstamos para empresas en sectores específicos o que se vieron afectadas por la crisis, por un total potencial de 72 billones (o el 6,8% del PIB de 2019). Para asegurar un apoyo fiscal adecuado, se activó la cláusula de suspensión de la regla fiscal para 2020 y 2021. En el frente monetario, el banco central recortó su tasa de intervención

en 250 puntos básicos entre marzo y septiembre y la redujo a su nivel histórico más bajo. Al mismo tiempo, introdujo una amplia gama de medidas para aumentar la liquidez.

Se prevé que estas medidas mitiguen el impacto en la economía del COVID-19. Sin embargo, con la contracción de la economía en 2020, se estima un repunte del crecimiento para 2021-2022, siempre que la pandemia sea de corta duración. Se espera que el entorno de bajas tasas de interés, facilitado por el banco central, impulse el crecimiento del consumo privado sujeto a como se suavicen las medidas de contención del COVID-19. También se espera que las bajas tasas de interés faciliten un repunte gradual de la inversión a medida que se reanuden importantes proyectos de infraestructura como las carreteras 4G y los proyectos del metro de Bogotá. Se espera que la inflación caiga hacia el límite inferior del rango establecido como objetivo por el banco central, ya que las presiones inflacionarias de la depreciación cambiaria se verán atenuadas por la débil demanda.

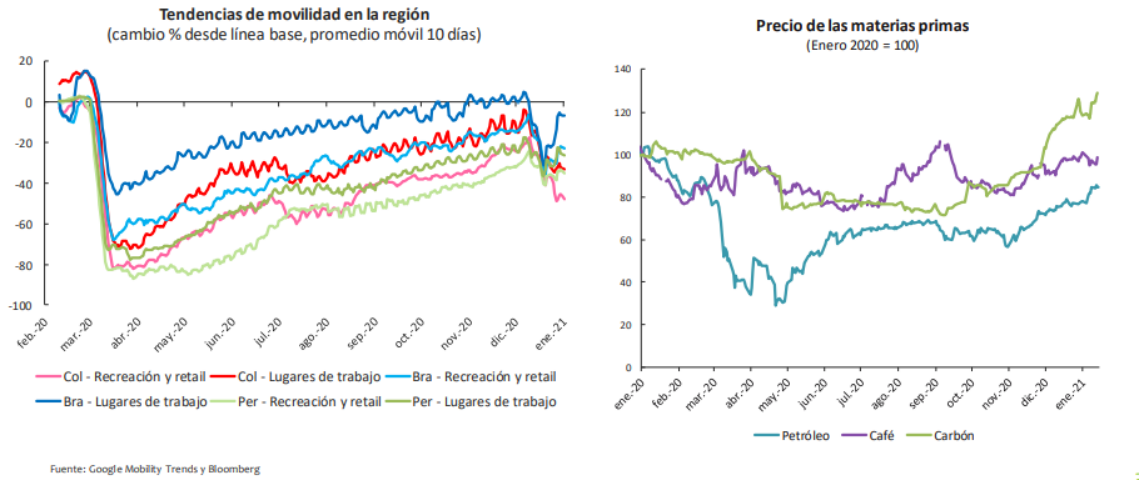
Se estima que los bajos precios del petróleo y las reducciones en la demanda global compensen la caída de las importaciones generada por la caída de la demanda doméstica. Por su parte, se espera que las fuertes entradas de remesas y los dividendos más bajos para los inversionistas extranjeros directos hagan que el déficit en cuenta corriente mejore ligeramente, desde el 4.2% del PIB en 2019 al 4,1% del PIB en 2020. También se estima que la normalización de los flujos comerciales y una mejora en el pago de dividendos a los inversores extranjeros directos provoquen un repunte del déficit en cuenta corriente en 2021, hasta que este se estabilice en 4,2% del PIB en 2022.

“Más allá del mediano plazo, las perspectivas dependen de la duración y gravedad de la crisis, la forma y la velocidad en la que se reducirá el déficit fiscal y la capacidad del país para abordar los cuellos de botella estructurales existentes.”[22]

Según el Banco de la República, la economía colombiana enfrentó un choque sin precedentes consecuencia de la pandemia y una disminución de los precios internacionales de los productos básicos.

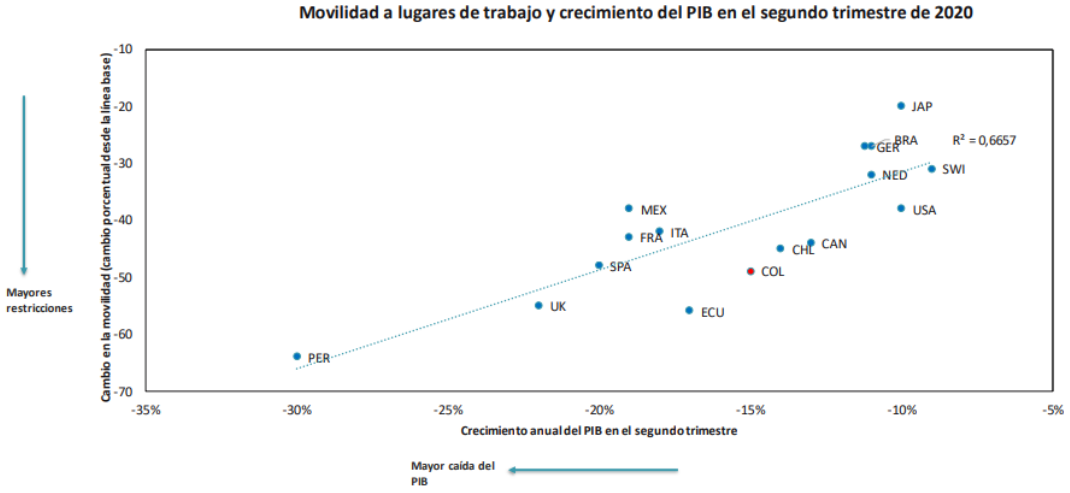
[22] https://www.bancomundial.org/es/country/colombia/overview#1

- **La economía colombiana enfrentó un choque sin precedentes** consecuencia de la pandemia y una disminución de los precios internacionales de los productos básicos.



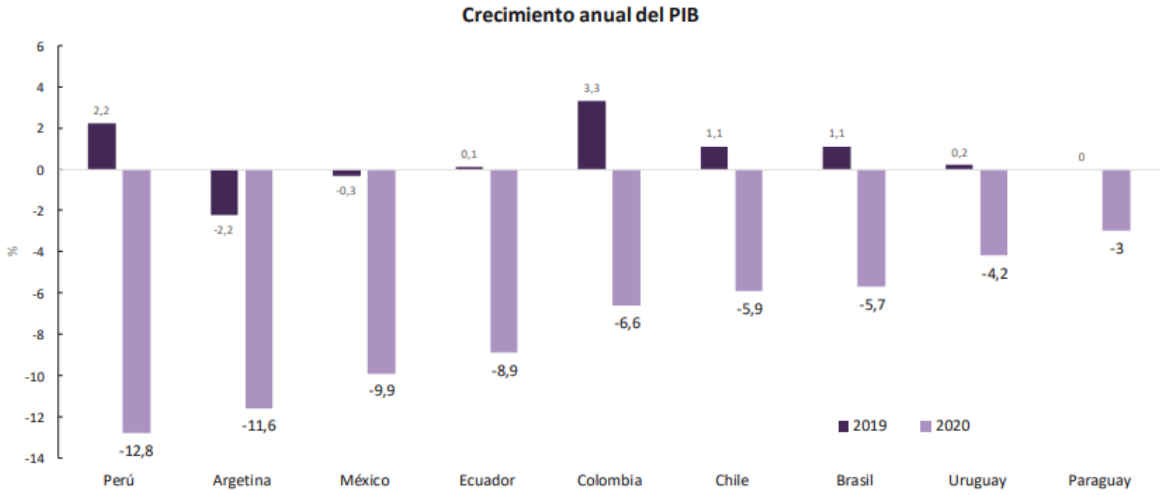
Fuente https://www.banrep.gov.co/sites/default/files/publicaciones/archivos/csoto-foro-mckinsey-22-01-2021.pdf

- La magnitud de la recesión está asociada a las medidas de salud pública implementadas para contener los contagios.



Fuente https://www.banrep.gov.co/sites/default/files/publicaciones/archivos/csoto-foro-mckinsey-22-01-2021.pdf

La caída del PIB en Colombia está en el promedio de la región:



Fuente https://www.banrep.gov.co/sites/default/files/publicaciones/archivos/csoto-foro-mckinsey-22-01-2021.pdf

4 ANÁLISIS DE LA OFERTA

Las organizaciones deben procurar ser cada día más eficientes, no solo en alcanzar más ventas y clientes dejándolos satisfechos, sino al interior de la organización tener los procesos depurados, frente a la asertividad y eficiencia de cada uno, un año inolvidable como el 2020 nos ha dejado grandes enseñanzas que debemos catapultar como oportunidades para el corto y mediano plazo. Regresemos a marzo del 2020, cuando el presidente Iván Duque, da inicio a la cuarentena obligatoria en Colombia, enfocándonos en las organizaciones, momento de validar la fortaleza de cada una, como estaba la madurez tecnológica para afrontar semejante reto, como estaban los indicadores tecnológicos de cada organización, entendiéndose los aspectos propios de las implementaciones tecnológicas como la capacidad, disponibilidad, ocupación, calidad de servicio, en general mediciones de carácter técnico que pueden ser obtenidas desde las diferentes plataformas mediante herramientas de gestión al interior de cada empresa y como se podría afrontar el trabajo remoto de los colaboradores.

El trabajo remoto da inicio a un gran reto para las empresas y es que las actividades que lleva a cabo un colaborador dentro de la organización tienen el objetivo de soportar un proceso, que puede estar o no oficializado o documentado, pero siempre nos indicará como se encuentra la información dentro del proceso organizacional.

Cuando se presentan las crisis, siempre surgen oportunidades; la Empresa para la Seguridad y Soluciones Urbanas – ESU ve una oportunidad al plantear un alcance mayor al objeto de la organización, llevándolo al tecnológico, para proveer herramientas a sus clientes que permitan mejorar sus procesos.

El Ministerio de Tecnologías de la Información y las Comunicaciones, según la Ley 1341 de 2009 “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”, 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. A continuación presentamos información acerca de las instituciones relacionadas con la formulación, ejecución y regulación de servicios en materia de tecnologías de la información y las comunicaciones en el país[23], y que dependen directamente del Ministerio de tecnologías de la información y las comunicaciones

- Colombia TIC Estadísticas
- Cifras
- Registro TIC

[23] http://www.mintic.gov.co

- Sector Postal
- Fiti
- Sector de Radiodifusión Sonora
- Espectro
- I+D+I
- RABCA
- Sistema de Gestión del Espectro (SGE)
- Venta de Equipos Terminales Móviles

Las instituciones relacionadas con el Ministerio de Tecnologías de la Información y las Comunicaciones que cumplen funciones de soporte y mejoramiento de procesos en el desarrollo de infraestructura, servicios y aplicaciones para beneficiar a usuarios y entidades sectoriales que aportan al crecimiento del país, son las siguientes:

- Agencia Nacional del Espectro (ANE)
- Autoridad Nacional de Televisión (ANTV)
- Radio Televisión de Colombia (RTVC)
- Señal Colombia – (Sistema de Medios públicos)
- Comisión de Regulación de Comunicaciones (CRC)
- Colciencias
- Red Postal de Colombia
- Computadores para Educar (CPE)

El Comando Conjunto Cibernético se desempeña como unidad élite en aspectos relacionados con la Ciberseguridad y Ciberdefensa, incluida la protección de las Infraestructuras Críticas Cibernéticas Nacionales, desarrollando operaciones militares en el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional, contribuyendo a generar un ambiente de paz, seguridad y defensa nacional. De otro lado, el organismo coordinador a nivel nacional de todos los aspectos de seguridad informática, ciberseguridad y ciberdefensa ColCERT tiene como misión la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

Por otra parte se tiene dentro de las funciones de la Superintendencia de Industria y Comercio, establecidas en el decreto 4886 de 2011 "*Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones",* la de "Velar por la observancia de las disposiciones sobre protección de la competencia; atender las reclamaciones o quejas por hechos que pudieren implicar su contravención

y dar trámite a aquellas que sean significativas para alcanzar en particular los siguientes propósitos: la libre participación de las empresas en el mercado, el bienestar de los consumidores y la eficiencia económica."

A continuación se relaciona las agremiaciones y asociaciones que participan en el sector de las tecnologías de la información y las comunicaciones:

- Asociación Colombiana de Ingenieros - ACIEM
- Asociación Colombiana de Ingenieros de Sistemas – ACIS-
- Asociación Colombiana de Usuarios de Internet – ACUI-
- Asociación Nacional de Empresas de Servicios Públicos Domiciliarios y Actividades Complementarias e Inherentes – ANDESCO-
- Asociación Nacional de Medios de Comunicación – ASOMEDIOS-
- Cámara Colombiana de Informática y Telecomunicaciones – CCIT-
- Centro de Investigación de las Telecomunicaciones – CINTEL-
- Federación Colombiana de la Industria de Software y Tecnologías Informativas Relacionadas – FEDESOFT-
- Asociación de Operadores de Tecnologías de Información y Comunicaciones de Colombia – ASOTIC.

Específicamente para los servicios de Seguridad de la Información y ciberdefensa no se cuenta con una asociación o gremio registrado en el MinTic.

Dentro de la investigación del tamaño del mercado, se pudo establecer que la asociación colombiana de ingenieros (ACIS) resume un número (160) considerable de empresas que prestan los servicios de seguridad informática. La cuales se pueden consultar en el siguiente link: https://acis.org.co/portal/content/lista-de-empresas-de-seguridad-inform%C3%A1tica-en-colombia

NOMBRE DE LA EMPRESA	SITIO WEB
0 Riesgos Consultores	https://sites.google.com/site/hadm88
360 Security Group S.A	www.360sec.com
360 Integral Security S.A.S.	www.360isg.com
2Secure S.A.S	www.2secure.org
A3SEC	www.a3sec.com
ACT Tecnología Informática	www.act.com.co
Activos TI SAS	www.activosti.com
Adalid Corp S.A.S	www.adalid.com

NOMBRE DE LA EMPRESA	SITIO WEB
Addintech	www.addintech.com
Adistec Colombia	www.adistec.com/co
Aerolen	www.arolen.com
Afina	www.afina.com.co
Antai Group Ltda	www.antai-group.com
Antifraude	www.antifraude.co
ASR Soluciones	www.asr-la.com
Assurance ControlTech SAS	www.ascontroltech.com
ASSURE IT SAS	https://assureit.co
ASTAF –TICS – División Tecnologías de la información y las comunicaciones	www.astaf.com
Azuan Technologies S.A	www.azuan.com
A&M Asesorías Integrales Ltda.	www.aymasesorias.com
BDO Audit S.A.	www.bdo.com.co/es/
Binary TI	www.binaryti.co
BLT Colombia	www.bltcolombia.com
B-Secure	www.b-secure.co
BSolution Group S.A.S.	www.bsolutiongroup.com
Centro de Soluciones Tecnológicas Siglo XXI	www.cstsigloxxi.com
CISCO (Security consulting)	www.cisco.com/global/CO
CLM Colombia S.A.S	www.clm.com.co
Cloud Seguro	www.cloudseguro.co
Complex Security Networks	www.complexsn.com
Consulting Network Security	www.cns.com.co
Consultores de sistemas de información CSI COLOMBIA	www.csi-internacional.com
CONTROL IT	www.controlit.com.co
Creange	www.creangel.com
Cross Border Technology	http://www.crossbordertech.com
CSIETE	http://www.csiete.org/
DATASECURE S.A.S	www.datasecure.com.co
Deloitte & Touche (Security services)	www.deloitte.com
Desca	www.desca.com
Dexpro S.A.S	www.dexpro.co
Digital Business DBX Ltda	www.digital01.com.co
Digiware S.A.	www.digiware.net
DragonJAR Soluciones y Seguridad Informática SAS	www.dragonjar.biz
DSTEAM Seguridad Informática	www.dsteamseguridad.com
Data y Service Limitada	www.datayservice.com/

NOMBRE DE LA EMPRESA	SITIO WEB
Easysolutions Inc.	www.easysol.net
EC Security Solutions SAS	www.ec-sec.com.co
Ecomil S.A.S.	www.solucionesecomil.com
Efeyce Integrales S.A.S	www.efeyceintegrales.com
Elliptical Ltda	www.elliptical.com.co
Enfocus	www.en-focus.com
Entelgy	www.entelgy.com
ERC Colombia SAS	www.erc.com.co/site
Ernest & Young (Riesgos en Tecnología y Seguridad)	www.ey.com/global
Estéganos International Group	www.esteganos.com
ETEK S.A.	www.etek.com.co
Everis	www.soceveris.com
Evolution Technologies Group	www.evolution-it.com.co
The Eagle Labs	www.theeaglelabs.com
Fast & ABS Auditores Ltda.	www.fastauditores.com
Fluidsignal Group	www.fluidsignal.com
FoxNet Sistemas Ltda	www.foxnetsistemas.com
Gamma Ingenieros S.A.	www.gammaingenieros.com
Global Crossing	www.globalcrossing.com
Globaltek Security	www.globalteksecurity.com
GMTECH	www.gmtech.es
Grupo ATLAS De Seguridad Integral	www.atlas.com.co
Grupo Oruss	www.grupooruss.com
Grupo Ultra	www.grupoultra.com.co
HACK-INN sas	www.hack-inn.com
Hack&Secure SAS	www.hackandsecure.net
HARDTECH S.A.S	www.hardtech.co
Human Hacking	www.humanhacking.com.co
IT Government Hambar	www.hambar.com.co
IBM (Servicios de Seguridad y Privacidad)	www.ibm.com/co/services/security
Icon Company	www.iconcompany.com
Identian	www.identian.co
IDISH	www.idish.com.co
Imaginanda	www.imaginanda.com.co
Indra / Minsait	https://www.minsait.com/es
Infocomunicaciones	www.infocomunicaciones.net
Information Security Systems - ISS	www.iss.com.co
Information Technology Security Solutions (ITSS) Ltda	www.itss.com.co

NOMBRE DE LA EMPRESA	SITIO WEB
Ingeniería Telemática S.A.S	www.ingenieriatelematica.com.co
Integrar S.A	www.integrar.com.co
Intergrupo S.A	www.intergrupo.com
InterLAN	www.interlan.com.co
Internet Security Auditors Colombia S.A.S.	www.isecauditors.com
Internet Solutions	www.internet-solutions.com.co
InterNexa S.A	www.internexa.com
IQ Information Quality	www.iqcol.com
Isec Information Security Inc	www.isec-global.com
IT Forensic SAS	www.itforensic-la.com
IT SECURITY	www.itsecurity.com.co
ITECH S.A.S	www.itechsas.com
Soluciones Inteligentes para Negocios Masivos - Inteligensa	www.inteligensa.com
J2K Security Group	www.j2ksec.com
Jupack IT Solutions	https://junpack.co
Kinetic Solutions	www.kineticsl.com
KPMG	www.kpmg.com.co
Kryptogénesis It Security	www.kryptogenesis.com.co
Latinus Ne	www.latinus.net
Lia Solutions Ltda	www.liacolombia.com
Locknet S.A.	www.lock-net.net
Mareigua	www.mareigua.com
MBA ® Gestión de Riesgos y Seguros	https://mbariesgos.com/
Millán C. & Asociados	www.millanyasociados.com
Micro Focus	https://www.microfocus.com/es-es/home
Mnemo	www.mnemo.com
Multisoft	www.multisoft.com.co
Némesis S.A.	www.nemesis.com.co
NeoSecure Colombia	www.neosecure.com
Neream	www.neream.com.co
Netdata Networks	www.netdatanetworks.com
NetSecure Colombia	www.netsecure.com.co
Network Security Team	www.nst.com.co
Newnet S.A.	www.newnetsa.com
Niterix	www.niterix.com
Nuvol Cybersecurity Services S.A	www.cybernuvol.com

NOMBRE DE LA EMPRESA	SITIO WEB
OBIKUZ S.A.S Integrador Tecnológico	www.obikuz.net
Olimpia	www.olimpiait.com
Ona Systems SAS	www.onasystems.net
Password Safe S.A.S	www.passwordsafesas.net
Password Seguridad Informática S.A.	www.password.com.co
PCM	www.pcm-ti.com
PricewaterhouseCoopers - PwC	www.pwc.com/co
PyP Servicios y Sistemas Integrados	www.pypservi.com
Red Colombia	www.redcolombia.com.co
Red Segura	www.redsegura.com
Ricardo Bernate y Compañia Ltda	www.rbcia.net
SAFETY IN DEEEP SAS	www.safeid-sas.com
S2 Grupo Colombia	www.s2grupo.co
Scientech - Seguridad e Inteligencia Informática	www.scientechsecurity.com
Sciotec s.a.s	www.sciotec.net
SecTorch S.A.S.	www.sectorch.com
Secure Information Systems s.a.s (GERSAFE)	www.gersafe.com.co
SecuriTIC Group	www.securitic.com.co
SeguraTec S.A.S	www.seguratec.com.co
Seltika, Seguridad Informática	www.seltika.com
Siemens S.A.	www.siemens.com.co/security
SISEL Ingeniería S.A.S.	www.siselingenieria.com
SlabInfo	www.slabinfo.com
Softnet S.A.	www.softnet.com.co
Software Channel - Symantec Partner	www.softwarechannel.net
SOLUCIONES EN SEGURIDAD INFORMATICA S.A.S	WWW.SEGURINFO.CO
Sotecsa Colombia S.A.S.	www.gruposotecsa.com
SSE Ltda	www.sse.com.co
SSP (Secure Solutions Provider)	www.securesolutionsprovider.com
SWAT Security IT	www.swatsecurityit.com
System Security Hardening	www.ssh-consulting.com
Systematic Solutions	www.systematicsolutions.com.co
SecPro Security Professionals	https://secpro.co/
Tecnología en Sistemas Avanzados	www.tsaconsultores.com.co
Teknii	www.teknii.com
Terremark	www.terremark.com.co
Trustwave	www.trustwave.com
TutaSec SAS	www.tutasec.com

NOMBRE DE LA EMPRESA	SITIO WEB
Unisys	www.unisys.com/unisys
Up Connection SAS	www.upconnection.co
Vilsol	www.vilsol.com

4.1 Estudio de la capacidad financiera y organizacional

INDICADOR	CÁLCULO	VALOR HABILITANTE
Indicador de Liquidez	$\frac{\text{Activo corriente}}{\text{Pasivo Corriente}}$	Mayor o igual a uno punto noventa y cinco (1.95)
Indicador de Endeudamiento	$\frac{\text{Pasivo total}}{\text{Activo Total}}$	Menor o igual al cincuenta y tres por ciento (53%)
Capital de trabajo	Activo Corriente - Pasivo Corriente	Mayor o igual a seis mil ochocientos ochenta millones de pesos M.L ($6.880.000.000)
Cobertura de Intereses	$\frac{\text{Utilidad operacional}}{\text{Gastos intereses}}$	Mayor o igual a dos punto cinco (2.5)
Rentabilidad del Patrimonio	$\frac{\text{Utilidad operacional}}{\text{Total Patrimonio}}$	Mayor o igual a cero punto diez (0.10)
Rentabilidad del Activo	$\frac{\text{Utilidad operacional}}{\text{Total Activos}}$	Mayor o igual al cero punto cero cuatro (0.04)

El sustento se encuentra en formato FT-MA-GCO-O4 denominado ESTUDIO DEL SECTOR: CAPACIDAD FINANCIERA Y ORGANIZACIONAL PARA PROPONENTES que hace parte integral del presente estudio.

5 ANÁLISIS DE LA DEMANDA

La Empresa para la Seguridad y Soluciones Urbanas - ESU, es una Empresa Industrial y Comercial del Estado, del orden municipal, que tiene por objeto brindar soluciones integrales de seguridad, tecnología, servicios de redes y telecomunicaciones para la gestión urbana y del riesgo a entidades del orden nacional e internacional, a través de la comercialización y prestación de bienes y servicios mediante alianzas, convenios, contratos, cooperación intersectorial y actividades permitidas por la Ley, para contribuir a la transformación social, la innovación, la investigación, el desarrollo económico y ambiental de las ciudades y territorios.

En cumplimiento de su objeto y de conformidad con lo dispuesto en el Acuerdo 090 de 2019, por el cual se adopta el reglamento de contratación de la ESU, la entidad podrá realizar selección de aliados proveedores mediante solicitud pública de oferta, con el fin de poder suministrar con eficiencia y eficacia los bienes y servicios que requieran sus clientes. La ESU no cuenta actualmente con aliados proveedores que garanticen la prestación de los servicios para atender las necesidades en materia de seguridad digital de los clientes, y con el objetivo de ofrecer nuevos servicios, cuenta con la nueva Línea Estratégica de Tecnología que fue incorporada a partir del acuerdo número 102 del 8 de marzo de 2021.

Por lo anterior, y en aras de prestar el servicio eficientemente, la ESU procederá con la convocatoria de aliados proveedores con las siguientes generalidades:

- Modalidad de contratación: Solicitud Pública de Oferta- SPO[24]
- Objeto: Selección de empresas comercializadoras de bienes y servicios de Soluciones de Seguridad Digital, Seguridad de la Información y Ciberseguridad como aliados proveedores para la firma de acuerdos marco con la Empresa para la Seguridad y Soluciones Urbanas – ESU.
- Cantidad: De acuerdo con el Sistema Electrónico de Contratación Pública – SECOP, varias entidades Públicas han adelantado procesos de selección referente al objeto que la entidad pretende contratar entre los años 2019 y 2020:

[24] Artículo 21. Procedimiento SPO – Acuerdo 090 de 2019

ITEM	ENTIDAD	OBJETO	No. PROCESO	FECHA PUBLICACIÓN	VALOR
1	CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL	Realizar las pruebas de seguridad establecidas en el alcance, con el fin de identificar las debilidades frente a posibles amenazas cibernéticas y así poder mitigarlas a través de controles que permitan una mejora continua en la operación de la agencia nacional digital.	CMA-AND-001-2021	25/03/2021	345.117.143
2	UNIDAD NACIONAL DE PROTECCIÓN	Adquirir una solución de protección de endpoint basado en edr (endpoint detection and response) y protección de correo para la unidad nacional de protección.	PSA-UNP-043-2021	24/03/2021	$619.345.140
3	SECRETARÍA DISTRITAL DE MOVILIDAD	Realizar la gestión y monitoreo de la seguridad informática sobre la plataforma tecnológica de la secretaría distrital de movilidad a través de un centro de operaciones de seguridad SOC.	SDM-LP-009-2021	5/03/2021	$857.779.648
4	Rama Judicial – Dirección Ejecutiva de Administración	Realizar la interventoría integral a los contratos que tienen por objeto prestar los servicios de conectividad, datacenter y seguridad perimetral y de audiencias virtuales y gestión de grabaciones	CM-07-2020-	11/11/2020	$1.581.283.400
5	MUNICIPIO DE MEDELLIN	Adquisición, Implementación, Suscripción al Soporte y Actualización de una Solución de Dispositivos de Seguridad Perimetral	9013981	5/11/2020	$1.458.808.429

ITEM	ENTIDAD	OBJETO	No. PROCESO	FECHA PUBLICACIÓN	VALOR
6	FONDO NACIONAL DEL AHORRO - FNA	Servicio integral de seguridad de la información enfocada en la gestión y manejo de incidentes, evaluación de vulnerabilidades, pruebas de intrusión, monitoreo de seguridad y evaluación de código fuente	FNA-SG-SB-002-2020	6/10/2020	$1.219.740.520
7	SERVICIO GEOLÓGICO COLOMBIANO	Contratar la adquisición, ampliación y renovación de licencias y hardware para la solución Mcafee y las licencias de una solución de gestión de vulnerabilidades (infraestructura y aplicaciones) del Servicio Geológico Colombiano	SGC-SA-SI-52-2020	2/10/2020	$3.750.435.194
8	AEROCIVIL	Prestar el servicio para el diseño, implementación y puesta en funcionamiento del servicio de gestión de seguridad tipo SOC (Security Operation Center).	20001084 H3 DE 2020	17/09/2020	$4.814.113.687
9	FISCALÍA GENERAL DE LA NACIÓN NIVEL CENTRAL	Actualización de la plataforma SIEM de la entidad – (grupo 1) y adquisición, configuración e instalación de un nuevo componente SIEM y SOAR (grupo 2) para el SOC de la Fiscalía General de La Nación	FGN-NC-IPSE-0029-2020	8/09/2020	$2.499.905.668

ITEM	ENTIDAD	OBJETO	No. PROCESO	FECHA PUBLICACIÓN	VALOR
10	MINISTERIO DE MINAS Y ENERGIA	Contratar la adquisición, instalación, configuración, implementación y puesta en marcha de una plataforma tecnológica tipo GRC (Gobierno, Riesgo Cumplimiento) de uso sectorial con licenciamiento, que permita hacer la administración, gestión, seguimiento, gobierno y monitoreo del sistema integrado de gestión de seguridad de la información y los sistemas de información tanto del Ministerio de Minas y Energía y sus entidades adscritas.	SMEC-182-CP-B-	25/08/2020	$1.509.937.189
11	INSTITUTO COLOMBIANO AGROPECUARIO - ICA	Diseño, instalación, configuración, administración, puesta en funcionamiento y gestión del servicio de seguridad de la información y ciberseguridad para el Instituto Colombiano Agropecuario	GC-LP-181-2020	21/07/2020	$2.000.000.000
12	DIRECCIÓN DE INTELIGENCIA POLICIAL	Adquisición sistema de ciberinteligencia basado en inteligencia artificial para la Dirección de Inteligencia Policial	PN DIPOL SA 042-2020	5/05/2020	$4.345.706.918
13	CENTRAL ADMINISTRATIVA Y CONTABLE TELEMATICA	Adquisición e implementación del sistema de sensores de red para el fortalecimiento de los medios cibernéticos del Ejército Nacional Fase II	LP-055-COADE-DICRE-CENAC-TELEMATICA-2020	13/04/2020	$2.803.453.616

ITEM	ENTIDAD	OBJETO	No. PROCESO	FECHA PUBLICACIÓN	VALOR
14	FONDO ÚNICO DE TIC	Prestar servicios de asistencia y apoyo especializado a las entidades públicas para promover buenas prácticas para la adopción, implementación y apropiación de la Política de Gobierno Digital y el impulso a los procesos de transformación digital.	FTIC-LP-011-2020	1/04/2020	$7.681.663.344
15	CVC - CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA	Servicios especializados de telecomunicaciones, networking y seguridad informática para la sede principal, las direcciones ambientales regionales (dar) y las subsedes de la CVC	LP 04 DE 2020	11/03/2020	$ 12.140.309.602
16	MINISTERIO DE CULTURA	Contratar los servicios de seguridad informática gestionada y administrada para el Ministerio de Cultura (Presentación de oferta)	MC LP 008 2019	26/08/2019	$ 3.333.333.056
17	FONDO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	Contratar el fortalecimiento de las herramientas de análisis y servicios tecnológicos de la entidad en materia de tecnología, informática y TIC asegurando una información oportuna y de calidad ofreciendo los mecanismos necesarios para el cumplimiento.	FTIC-LP-010 de 201	2/08/2019	$10.390.364.567
18	REGISTRADURÍA NACIONAL DEL ESTADO CIVIL (RNEC)	Prestar el servicio de una solución informática integral para la Seguridad de la Información del proceso electoral que garantice la confidencialidad, integridad y disponibilidad de la información a gestionar en el desarrollo de las elecciones de Autoridades Territoriales a realizarse en el año 2019.	014 DE 2019 RNEC	30/07/2019	$ 5,219,205,000

ITEM	ENTIDAD	OBJETO	No. PROCESO	FECHA PUBLICACIÓN	VALOR
19	SUPERINTENDENCIA DE SERVICIOS PÚBLICOS DOMICILIARIOS	Adquisición, puesta en producción y soporte de una solución integral de seguridad informática de última generación, que fortalezca la confidencialidad, integridad y disponibilidad de la información que maneja la Superintendencia de Servicios Públicos Domiciliarios	SSPD-SA-008-2019	19/07/2019	$ 1.999.889.304
20	INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR (ICBF)	Servicios de Tecnología de la Información y Comunicaciones (TIC) bajo la modalidad de Outsourcing para la administración de la Infraestructura Tecnológica de la Entidad, incluidas las actividades de administración, gestión, operación, monitoreo y control especializado de la plataforma de Almacenamiento, Respaldo, Servidores, Aplicaciones, Bases de Datos, Office 365, Seguridad Informática y de la Información, Centro de Operaciones de Seguridad (SOC), Redes LAN y Redes Inalámbricas, Correo Electrónico, servicio de administración del Centro de Cómputo de la Sede Nacional, servicios agregados y conexos, para el Instituto Colombiano de Bienestar Familiar (ICBF).	sa0092016sen	16/11/2016	$ 14,017,162,322

JAIRO ANDRÉS LONDOÑO PARDO
Subgerente de Servicios

Aprobó: Juan Felipe Hernández Giraldo- Secretario General
Aprobó: Jairo Andrés Londoño Pardo - Subgerente de Servicios
Aprobó: Marelbi Verbel Peña- Subgerente Administrativa y Financiera.
Revisó: Edison Osorio Hernández. Profesional Especializado Unidad de Gestión Jurídica
Proyectó: Mauricio Alejandro Patiño Restrepo. Líder de Programa. Unidad Estratégica de Servicios SIS