DISTRISEGURIDAD

TECNOLOGÍA, PREVENCIÓN, ARTICULACIÓN

Sistema Integrado de Gestión

PLAN ESTRATEGICO DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES - PETI

Código: MGTICS - 003

CARTAGENA DE INDIAS D. T. y C, 20 DE ENERO DE 2023

Este Plan Institucional fue socializado y aprobado mediante acta de Comité de Gestión y Desempeño – MIPG realizado los días 23 y 26 de enero de la presente vigencia.

Plan Estratégico de Tecnologías de la Información – PETI

De acuerdo al Marco de Referencia de Arquitectura Empresarial para la Gestión de TI del Estado colombiano, el Plan Estratégico de las Tecnologías de la Información y Comunicaciones (en adelante PETI) es el artefacto que se utiliza para expresar la Estrategia de TI. El PETI hace parte integral de la estrategia Distriseguridad y es el resultado de un adecuado ejercicio de planeación estratégica de TI. Cada vez que la institución pública haga un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.

1. Objetivos Específicos

- Mejorar los servicios tecnológicos que tiene Distriseguridad actualmente.
- Implementar estratégicamente sistemas de información que puedan beneficiar a la población misional de Distriseguridad.
- Innovar en Distriseguridad, mediante nuevas tecnologías estables, la parte operacional como misional de Distriseguridad.
- Desarrollar la Arquitectura Empresarial de Distriseguridad bajo los criterios de Gobierno en Línea.
- Mejorar los componentes de seguridad del dominio del marco referencial para Distriseguridad.
- Definir el mapa de ruta del PETI para Distriseguridad.
- Desarrollar lineamientos para orientar el crecimiento, mantenimiento y fortalecimiento TI del sector.

2. Alcance del documento

El Plan de Desarrollo 2019 de Distriseguridad considera los lineamientos de política de TIC aprobados en las bases del Plan Nacional de Desarrollo 2018 – 2022 "Pacto por Colombia, Pacto por la Equidad" a través de la Ley 1055 de 2019

Planes regionales de tecnologías de la información y las comunicaciones. El Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) incluirán programas regionales de Tecnologías de la Información y las Comunicaciones (TIC), en coordinación con Colciencias y otras entidades del Estado. Dichos planes estarán alineados con los objetivos del Plan Nacional de Desarrollo.

3. Marco Normativo

El plan estratégico de las tecnologías de información aplicado a Distriseguridad se encuentra directamente relacionado a la normativa nacional colombiana, por tal razón es compromiso de esta entidad seguir detalladamente las pautas que presenta el MINTIC para las entidades del estado.
En la siguiente tabla, se presentan las normas a considerar aplicables con respecto a la elaboración del documento PETI y otras regulaciones relevantes de Distriseguridad en el tema tecnológico.

Norma	Descripción
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Decreto 1122 de 1999	Por el cual se dictan normas para suprimir trámites, facilitar la actividad de los ciudadanos, contribuir a la eficiencia y eficacia de la Administración Pública y fortalecer el principio de la buena fe.
Decreto 1151 de 2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
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.
Ley 1581 del 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341

	de 2009 y 1450 de 2011, y se dictan otras disposiciones.
Ley 1712 del 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 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 0103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de tecnología de la Información y las Comunicaciones
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

4. Rupturas Estratégicas

Las rupturas estratégicas nos permiten identificar los paradigmas a romper de la Institución pública para llevar a cabo la transformación de la gestión de TI, a continuación, se listan las siguientes rupturas estratégicas identificadas:

- Distriseguridad debe ver la tecnología como un valor estratégico para la Estrategia de la Seguridad en la Información.
- Alinear las soluciones con los procesos, aprovechando las oportunidades de la tecnología, según el costo/beneficio.
- Los sistemas de información no se integran y no facilitan las acciones coordinadas.
- Se debe minimizar la brecha entre los directivos y el personal de TI.
- Las direcciones territoriales deben estar integradas al Nivel Central desde lo tecnológico.

• Ausencia de capacidad de análisis debido al poco conocimiento del dominio de información.

5. Análisis de la Situación Actual

Distriseguridad está trabajando en el éxito sostenido de la estrategia Gobierno en Línea, la cual busca construir un Estado más eficiente, más transparente y más participativo mediante el uso de las TIC, prestando mejores servicios en línea, mayor participación ciudadana para empoderar y trabajando con mayor transparencia para generar confianza en los ciudadanos, así como impulsar las acciones requerida para avanzar en los Objetivos de Desarrollo Sostenible – ODS, facilitando el goce efectivo de derechos a través del uso de TIC.

5.1.1 Plan nacional de desarrollo:

En el Plan de Desarrollo 2019 de Distriseguridad se deben considerar los lineamientos de política de TIC aprobados en las bases del Plan Nacional de Desarrollo 2014 – 2018 "Todos por
un nuevo país" a través de la Ley 1753 de 2015 Capítulo VII - Estrategia territorial: ejes articuladores del desarrollo y prioridades para la gestión territorial.

(…) Artículo 195. Planes regionales de tecnologías de la información y las comunicaciones. El Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) incluirán programas regionales de Tecnologías de la Información y las Comunicaciones (TIC), en coordinación con Colciencias y otras entidades del Estado. Dichos planes estarán alineados con los objetivos del Plan Nacional de Desarrollo (…)

Dados los lineamientos brindados para el sector TIC a nivel nacional, así como para otros sectores económicos estratégicos para la economía y el beneficio social del país, y tomando en cuenta la oferta institucional del Gobierno Nacional, con énfasis en Programas del Ministerio de TIC como Dirección de Conectividad, Gobierno en Línea, Dirección de Promoción de TIC, así como los proyectos relacionados con la apropiación de TIC, nos permitimos proponer el siguiente texto como insumo para el Plan de Desarrollo de Distriseguridad.

En este sentido, Distriseguridad trabajará de la mano con el Ministerio de Tecnologías de la Información y las Comunicaciones (Ministerio TIC) para implementar estrategias conjuntas que permitan un adecuado acceso, uso y apropiación de las TIC, Lo cual impulsará el desarrollo endógeno y la competitividad del territorio.

Teniendo en cuenta nuestra política seguridad digital pretendemos:

La Entidad descentralizada Distriseguridad establecerá la seguridad digital como una responsabilidad institucional y un compromiso de todo el personal, liderada por el Equipo de Gestión TIC.

La Oficina Asesora de Planeación, el Equipo de Gestión Documental y El Equipo de Gestión TIC, revisará y actualizará los activos de información y en ello tendrá en cuenta la clasificación según su naturaleza, como por ejemplo, información, software, hardware y/o componentes de red.

El Equipo de Gestión TIC, hará el levantamiento de la Infraestructura Tecnológica Crítica de la Entidad.

El Equipo de Gestión TIC, actualizará los riesgos de seguridad digital, siguiendo la metodología dispuesta por el DAFP y el Ministerio de TIC.

El Equipo de Gestión TIC implementará el Modelo de Seguridad y Privacidad de la Información MSPI con las herramientas que el Ministerio de TIC destine para ello, el cual integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital.

El Equipo de Gestión TIC establecerá los controles definidos en el Anexo A de la ISO 27001:2013, que en el MSPI se define como la Declaración de Aplicabilidad.

El Equipo de Gestión TIC evaluará el desempeño del Modelo de Seguridad y Privacidad de la Información MSPI, a través de la aplicación de la política de seguridad y privacidad de la información, la ejecución de los controles definidos en la declaración de aplicabilidad y el monitoreo de los indicadores de seguridad de la información.

.

En el presente año se pretende:

Generar las condiciones para que el sector de las telecomunicaciones aumente su cobertura a través del despliegue de infraestructura, se amplíe la penetración de banda ancha, se intensifique el uso y la apropiación de las TIC.

Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más, más Eficiente transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad.

Cumplir con el Decreto 2573 de 2014 en la correcta implementación de la estrategia Gobierno en línea en cuanto a la implementación de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos, en condiciones de calidad, facilidad de uso y mejoramiento continuo; Fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones; Planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información.

Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno y proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada.

De esta forma lograr una gestión pública efectiva y orientada al servicio al ciudadano, a través de la modernización de la infraestructura administrativa pública, los modelos de gestión, entre ellos el de talento humano, el jurídico, y el archivo, y el uso de herramientas tecnológicas. Además, se logrará la efectividad, transparencia y oportunidad en los procesos de contratación.

5.1.2 Definición de los objetivos estratégicos de TI

• Integrar los sistemas de información de las diferentes áreas de Distriseguridad que permitan la toma de decisiones sostenibles y eficientes.

• Incentivar la competitividad y la innovación de la ciudad a través del empoderamiento y la confianza de los funcionarios en el uso de TIC.

• Fortalecer la gestión de las tecnologías de la información y comunicaciones (TIC), que permita la adopción de los estándares y lineamientos de la arquitectura empresarial para un desarrollo incluyente, sostenido, participativo y transparente dentro de Distriseguridad.

• Implementar el sistema de gestión de servicio para gestionar de manera formalizada los requisitos del cliente, las demandas del negocio convirtiéndolas en servicios de TI, de acuerdo con la estrategia y el presupuesto.

• Implementar sistemas de comunicación internos que permitan mejorar el nivel de interacción entre funcionarios y uso de las herramientas electrónicas para disminuir el uso de papel y aligerar la gestión documental.

• Implementar sistemas de participación externa que permitan mejorar el nivel de interacción entre la ciudadanía y los funcionarios, permitiendo influir en la toma de decisiones.

5.2 Uso y Apropiación de la Tecnología

Distriseguridad debe desarrollar cultura que facilite la adopción de tecnología es esencial para que las inversiones en TI sean productivas; para ello se requiere realizar actividades de fomento que logren un mayor nivel de uso y apropiación.

Para fomentar el uso y apropiación de la tecnología es necesario tener en cuenta:

- Garantizar el acceso a todos los públicos
- Usabilidad
- Independencia del dispositivo y de la ubicación
- Acceso a la red

Para ejecutar la estrategia de uso y apropiación de la oferta de sistemas y servicios de información debe tener en cuenta los diferentes aspectos públicos e implica adelantar actividades de:

- Capacitación
- Dotación de tecnología o de fomento al acceso
- Desarrollar proyectos de evaluación y adopción de tecnología
- Evaluación del nivel de adopción de tecnología y satisfacción en el uso.

Es preciso contar con herramientas de diferentes niveles: básicas, analíticas y gerenciales.
También se deben definir y aplicar procesos para comunicar, divulgar, retroalimentar y gobernar el uso y apropiación de TI. Todo esto con el objetivo principal de construir una administración de alto desempeño con las personas, para que TI sea un factor de valor estratégico.
Las premisas que soportan el componente de uso y apropiación de IT4+ buscan que entre los actores (funcionarios, ciudadanos, decisores, proveedores de TI, entre otros) se genere una cultura digital personal; que les permita interiorizar el Modelo IT4+ y sus componentes, como parte de su visión frente a la tecnología y la información. De igual manera, propicia de forma continua la adopción de diferentes elementos para lograr el uso y la apropiación de los productos y beneficios que brindan los demás componentes:

Gobierno de TI, Estrategia de TI, Gestión de Información, Sistemas de Información y Servicios Tecnológicos, los cuales se integran a los procesos de gestión de tecnología de cada entidad.

5.3 Sistemas de Información

Como parte del ejercicio de diagnóstico, se ilustrará el Inventario de equipos de cómputo, periféricos y sistemas de Información de Distriseguridad, teniendo en cuenta la categorización definida en el dominio de sistemas de información del marco de referencia.

Equipo de Oficina	Presencia	Licencia antivirus	Licencia de Office
Computadores de mesa completo	15	SI	SI
Portátiles	2	NO	NO
Impresora	8	N/A	N/A
Escáner	2	N/A	N/A
VideoBeam	2	N/A	N/A

Arquitectura Tecnológica

La arquitectura tecnológica actual de Distriseguridad está soportada en 2 ejes fundamentales con cuales es posible el acceso, la integración y despliegue de los servicios tecnológicos de la información y comunicaciones, se describen a continuación:

Arquitectura de procesamiento y almacenamiento

A nivel de servidores se necesita un servidores físicos, se espera en el corto plazo fortalecer la infraestructura de servidores de tal forma que se puedan establecer mecanismos que propendan la optimización del proceso y al tiempo que se mejoren los controles de acceso y la seguridad a la zona de comunicaciones y de servidores.

Arquitectura de red

Distriseguridad cuenta con una infraestructura de red inalámbrica y alámbrica para comunicaciones de datos en su oficina, soportada sobre tecnologías CISCO, TP-Link y 3Com.

Actualmente el ancho de banda instalado en la sede principal de Distriseguridad es de 200 Mbps sobre los cuales operan servicios de Internet y Web Services del sistema de información tributaria, mientras que en las otras sedes operan servicios de banda ancha los cuáles podrían ser migrados a servicios en fibra óptica en el mediano plazo.

Esta arquitectura está soportada por los equipos de red cableada, red inalámbrica.

La arquitectura tecnológica es la base fundamental que soporta las arquitecturas de aplicaciones, datos, procesos y finalmente gobierno electrónico.

5.4 Servicios Tecnológicos

Distriseguridad toma como referencia la metodología ITIL para empezar a gestionar sus servicios.

Teniendo en cuenta la estructura organizacional de Distriseguridad, se escogieron una serie de procesos, los cuales están basados en ITIL 2011 y se espera implementar a lo largo de la vigencia del presente plan.

Estrategia del Servicio

Gestión de la Relación con la Ciudadanía: Este proceso está enfocado en mantener una relación positiva con la ciudadanía, Identificar sus necesidades existentes y potenciales y asegurar que los servicios desarrollados sean apropiados para cumplir sus necesidades, (Diseño del Servicio).

Gestión del Catálogo de Servicios: Contiene información precisa y actualizada de todos los servicios operacionales y de los próximos a ofrecerse. La gestión de este catálogo provee información fundamental para el resto de los procesos de Gestión de Servicios (detalles de servicios, estatus actual e interdependencia de los mismos).

Gestión de Niveles de Servicios: Su función es negociar Acuerdos de Nivel de Servicio (SLA) con los clientes y diseñar servicios de acuerdo con los objetivos propuestos. La Gestión del Nivel de Servicio (SLM) también es responsable de asegurar que todos los Acuerdos de Nivel Operacional (OLA) y Contratos de Apoyo (UC) sean apropiados, y de monitorear e informar acerca de los niveles de servicio.

Gestión de la Disponibilidad: En este proceso se debe definir, analizar, planificar, medir y mejorar la disponibilidad de servicios de TI en todos los aspectos. La Gestión de la Disponibilidad se encarga de asegurar que la infraestructura, los procesos, las

herramientas y las funciones de TI sean adecuados para cumplir con los objetivos de disponibilidad propuestos para el negocio.

Gestión de la Capacidad: Asegura que la capacidad de servicios de TI y la infraestructura de TI sean capaces de cumplir con los objetivos acordados de capacidad y desempeño de manera económicamente efectiva y puntual. La Gestión de la Capacidad toma en cuenta todos los recursos necesarios para llevar a cabo los servicios de TI, y prevé las necesidades de la organización a corto, medio y largo plazo, (Transición del Servicio). Gestión de la Configuración de Activos y Conservación de la información acerca de Elementos de Configuración (CI) requeridos en la prestación de un servicio de TI, incluyendo las relaciones entre los mismos.

Gestión del Cambio: Su principal función es la evaluación y planificación del proceso de cambio para asegurar que, si éste se lleva a cabo, se haga de la forma más eficiente, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio TI.

Gestión del Conocimiento: Recopila, analiza, archiva y comparte conocimientos e información dentro de una organización. El propósito primordial de esta gestión es mejorar la eficiencia reduciendo la necesidad de redescubrir conocimientos. Operación del Servicio.

Gestión de Incidentes: Maneja el ciclo de vida de todos los Incidentes desde que inician hasta que se cierran. El objetivo principal del manejo de incidentes es devolver el servicio de TI a los usuarios lo antes posible.

Gestión de Problemas: Los objetivos primordiales de la Gestión de Problemas son la prevención de Incidentes y la minimización del impacto de aquellos Incidentes que no pueden prevenirse. La Gestión Proactiva de Problemas analiza los Registros de Incidentes y utiliza datos de otros procesos de Gestión del Servicio de TI para identificar tendencias o problemas significativos. Perfeccionamiento Continuo del Servicio.

Evaluación de Servicios: Evalúa la calidad de servicio regularmente. Esto incluye la identificación de áreas en que no se cumplen los niveles de servicio propuestos, y las conversaciones regulares con las empresas para asegurar que los niveles de servicio propuestos operen de acuerdo a con sus necesidades

Estrategia y gobierno:

• El ingeniero TIC es quien asesora y guía a la entidad en los temas de tecnología de la información y las comunicaciones de forma centralizada.

• El ingeniero TIC es el responsable de construir los lineamientos y políticas de la entidad para la implementación y uso de tecnologías que requiera el Ministerio de TIC.

• El ingeniero TIC es el responsable de articular el sector trabajo desde el componente tecnológico, así como de definir los mecanismos de relación con las demás entidades públicas y privadas que van a interactuar con el Ministerio de TIC.

• La estrategia de Distriseguridad es generar una arquitectura basada en el marco de referencia de Mintic a través de la estrategia Gobierno en Línea, para ajustar las falencias y mejorar los procesos en pro de la de una administración tecnológicamente optimizada.

5.5 Gestión de Información

Para los proyectos en el presente PETI se realizará el diagnóstico de la arquitectura de información, realizando un aprovechamiento de los componentes de información que se pueden reutilizar para hacer una integración de la información que sea beneficiosa para la entidad, para el sector y para el ciudadano.

Distriseguridad aplica el siguiente ciclo de inteligencia, donde se Orienta las acciones de recolección y procesamiento de información con el propósito de integrarlas en productos de inteligencia para los procesos de toma de decisiones. Comprende las siguientes etapas:

CICLO DE INTELIGENCIAPARA LA RECOLECCIÓNY PROCESAMIENTODE LA INFORMACIÓN DE DISTRISEGURIDAD

Planeación: En esta etapa se establecen las prioridades de los requerimientos de información estratégica, táctica y operativa, los cuales se traducen en planes de recolección que detallan las estrategias a seguir para cada caso.

Recolección: Durante esta etapa se ponen en marcha las actividades de recolección de información a partir de diversas fuentes con base en las solicitudes formuladas durante la fase de planeación.

Procesamiento y Análisis: La información obtenida en la etapa de recolección se depura, estandariza y, en su caso, se decodifica con el objeto de presentarla en un formato útil para las labores de análisis, cuyo propósito consiste en transformar la información en bruto en productos de inteligencia estratégica, táctica u operativa destinados a satisfacer necesidades de información específica.

Difusión y Explotación: El carácter confidencial de la información, así como la importancia de remitirla oportunamente a las personas indicadas, hacen que esta etapa sea de especial relevancia.
Con el fin de garantizar la seguridad de la información y evitar que caiga en manos equivocadas, los productos de inteligencia son objeto de una serie de procesos y medidas de seguridad con el propósito de evitar riesgos durante su traslado y entrega. Asimismo, durante esta etapa, se pone especial atención en hacer llegar la información con oportunidad a las personas indicadas antes de que sea demasiado tarde para los procesos de toma de decisiones.

Retroalimentación: Un aspecto de gran relevancia para el ciclo de inteligencia consiste en determinar el grado en que la información proporcionada atendió las necesidades de los procesos de toma de decisiones, o en su caso, si las personas a las que se les entrego la información requieren precisar o ampliar la información sobre un tema en especial. Lo que, en consecuencia, da inicio a las actividades de planeación y a comenzar nuevamente en la primera fase del ciclo de inteligencia.

6. ENTENDIMIENTO ESTRATÉGICO

Las tecnologías de la información y las comunicaciones son herramientas indispensables para la transformación productiva de la región, de la región, pues constituyen un apoyo transversal a los sectores que jalonarán la economía local para generar dinámica e innovación, aumentar la productividad y mejorar en competitividad. Así mismo, las TIC contribuyen a generar, transmitir y potenciar la creación de conocimiento –en particular ciencia y tecnología- constituyéndose en uno de los habilitadores centrales para la generación de la innovación. Facilitar y fomentar el uso y adaptación de tecnología son requisitos fundamentales para que la innovación en el país evolucione hacia la frontera del conocimiento.

Una ampliación de la cobertura en acceso a TIC implica un mayor Producto Interno regional. El Banco Mundial (2009) estima que por cada 10% de incremento en la penetración fija o de incremento en la penetración móvil se genera un incremento del 0,73% o del 0,81% respectivamente en el Producto Interno Bruto (PIB) de un país en vía de desarrollo. También se estima que el desarrollo de la banda ancha generaría un impacto relativo más alto que aquel generado por la telefonía fija o la telefonía móvil tanto para países en vía de desarrollo como para países desarrollados, alcanzando niveles similares y superiores al 1,2% de incremento en el PIB por un 10% de incremento en la penetración.

En este sentido se presentan lineamientos de política para el sector TIC a nivel local y regional, en articulación con la Política TIC a nivel nacional, en particular con el Plan Nacional de Desarrollo y el Plan Vive Digital para la gente, que permitan la inclusión digital de toda la población, personas con discapacidad, tercera edad, etnias, y demás grupos sociales; dichos lineamientos se enmarcan en la superación de brechas digitales, tanto en el nivel de infraestructura, como en la disponibilidad de dispositivos y terminales; y a la generación de aplicaciones y contenidos, buscando la apropiación generalizada de las TIC.

De esta manera, se implementará estos lineamientos de política, cuyo objeto es impulsar la masificación y uso de internet a través del desarrollo y uso eficiente de infraestructura, la promoción y apropiación de los servicios TIC, el desarrollo de aplicaciones, contenidos digitales y el impulso a la apropiación por parte de éstos. Con esto se busca consolidar el Ecosistema Digital Regional (infraestructura TIC, servicios, aplicaciones y usuarios) para la inclusión social y la disminución de la brecha digital, así como para la innovación, la productividad y la competitividad.

Por lo anterior, el presente plan de desarrollo encuentra pertinente y necesario para el desarrollo incluyente de Distriseguridad que las estrategias regionales para el desarrollo de las TIC guarden relación con las metas del Plan Vive Digital para la gente. En este sentido, Distriseguridad trabajará de la mano con el Ministerio de Tecnologías de la Información y las Comunicaciones (Ministerio TIC) para implementa estrategias conjuntas que permitan un adecuado acceso, uso y apropiación de las TIC en él. Este trabajo coordinado impulsará el desarrollo endógeno y la competitividad del territorio.

6.1 OBJETIVOS DE CALIDAD

- Aumentar los niveles de satisfacción de los ciudadanos en la sede virtual (Pagina web).

- Fortalecer el desempeño de los procesos establecidos en Distriseguridad.

• Garantizar la disponibilidad y el uso eficiente de los recursos financieros y el desarrollo integral de Distriseguridad.

• Garantizar mecanismos de participación ciudadana y control social sobre la gestión de Distriseguridad.

• Utilizar de manera eficiente los recursos ambientales.

6.2 Modelo operativo

Distriseguridad tiene implementado un modelo de operación por procesos el cual permite una mejor articulación entre las dependencias bajo una visión sistemática orientada al ciudadano.

El proceso de administración Tecnologías de la información es un proceso transversal que debe ubicarse en el macro proceso de Apoyo y debe "Garantizar de forma permanente y oportuna la disponibilidad, integridad, reserva, confidencialidad y resguardo de los datos y la información de la administración, mediante la políticas de gestión de seguridad de la información y el seguimiento para su aplicación; la búsqueda constante del uso de nuevas tecnologías y el soporte tecnológico de los sistemas, estructuras y equipos que almacenan, manejan y transportan los datos y la información, para acercar al usuario a la Administración Central utilizando sus diferentes servicios y facilitar a los colaboradores la ejecución de operaciones institucionales".

Con el fin de cumplir con el objetivo se debe documentar los siguientes procedimientos operativos:

- Implementación de sistemas de Información.
- Mantenimiento y Administración de sistemas de información.
- Administración de Infraestructura Tecnológica.
- Administración del Centro de datos.
- Administración de Telecomunicaciones.
- Seguridad Informática Perimetral.
- Soporte Tecnológico.

6.3 Necesidades de información

Distriseguridad debe acoger un conjunto de actividades y tareas que conllevan a la adecuada determinación de los requerimientos de información de un área o grupo de la entidad.

Para realizar tal identificación, se debe capturar la información, cuya estructura permita:

1. Identificar los lineamientos específicos que soportan la producción de información estadística en los organismos de Distriseguridad.

2. Relacionar las funciones que las normas y leyes señalan como misión, acción, políticas públicas, planes, programas y proyectos, que generan una responsabilidad en la producción de información, con el fin de generar un balance de la actividad estadística de Distriseguridad.

3. Identificación de los procesos, subprocesos y procedimientos vinculados a las normas y leyes para establecer y documentar los flujos de la información estadística en Distriseguridad.

4. Identificación y definición del alcance de los requerimientos que se deben establecer en la producción de información estadística; sus características y las áreas o grupos productores de información con sus responsables en cada una de las áreas.

6.4 Alineación de TI con los procesos Estructura del Plan Estratégico de TI Guía Técnica:

Atendiendo los lineamientos recomendados por el Mintic, Distriseguridad se propone implementar el modelo de gestión IT4+, el cual es un modelo construido a partir de la experiencia, de las mejores prácticas y lecciones aprendidas durante la implementación de la estrategia de gestión TIC en los últimos 10 años. IT4+® es un modelo integral de gestión estratégica con tecnología cuya base fundamental es la alineación entre la gestión de tecnología y la estrategia sectorial o institucional. El modelo facilita el desarrollo de una gestión de TI que genera valor estratégico para la del sector, la entidad, sus clientes de información y usuarios. Está conformado por los siguientes componentes: Estrategia de TI, Gobierno de TI, Análisis de información, Sistemas de información, Gestión de servicios tecnológicos, Apropiación y uso, los cuales abordaremos de forma más detallada en las siguientes secciones.

6.4.1 Definición de apoyo tecnológico a los procesos:

Apoyo en planes de mejoramiento de la organización con TI: En el compromiso de mejoramiento continuo de la administración pública, el área de TI debe incluir en su planeación actividades que conduzcan al corregir, mejorar y controlar los procesos que se hayan establecido en estado de no conformidad en el marco de las auditorias de control internas y externas. En la medida que la tecnología apoye los procesos del sector y de la entidad, la participación del área de TI en la implementación y seguimiento a los planes de mejoramiento de la entidad es mayor. Por tanto, el liderazgo que ejerce el área en estos procesos también es necesario para el cumplimiento de los planes establecidos.

Los sistemas de información se crean para soportar los procesos de la institución y en ese sentido, la alineación con los procesos de la entidad es vital. No obstante, si no hay una definición de procesos de gestión con estándares de calidad; se corre el riesgo de sistematizar malas prácticas. Por ejemplo, que los sistemas no estén adecuados a los requerimientos de la institución y que estén por debajo de los niveles de uso esperados.

Es frecuente encontrar que los sistemas de información no responden a los procesos o se quedan cortos en sus funcionalidades o bien tienen módulos que pudiendo ser útiles, no se utilizan, a pesar de estar disponibles, todo esto a causa de: una desalineación de los sistemas con los procesos, - deficientes procesos de levantamiento de los requerimientos y análisis de necesidades. La inexistencia de procesos hace muy complejo desarrollar los sistemas, pues su desarrollo requiere de unos fines comunes que sean adecuados a las actividades diarias. En un proceso de arquitectura empresarial o institucional, el éxito de su implementación depende de la forma como se integran los procesos con el apoyo tecnológico que requieren. Los dos aspectos son abordados en paralelo para que se diseñen de manera articulada y se realicen los ajustes necesarios en cada uno de ellos durante los momentos clave del proceso, tomando las decisiones oportunamente.

Apoyo en planes de mejoramiento de la organización con TI: En el compromiso de mejoramiento continuo de la administración pública, el área de TI debe incluir en su planeación actividades que conduzcan al corregir, mejorar y controlar los procesos que se hayan establecido en estado de no conformidad en el marco de las auditorias de control internas y externas. En la medida que la tecnología apoye los procesos del sector y de la entidad, la participación del área de TI en la implementación y seguimiento a los planes de mejoramiento de la entidad es mayor. Por tanto, el liderazgo que ejerce el área en estos procesos también es necesario para el cumplimiento de los planes establecidos.

7 MODELO DE GESTIÓN DE TI

7.1 Estrategia de TI

A continuación y siguiendo con el modelo de estrategia de TI, se realiza un direccionamiento organizacional en el cual se alinea la estrategia de TI con la estrategia institucional, la arquitectura empresarial o institucional se alinea con los mecanismos de Gobierno de TI, a través de políticas, acuerdos de desarrollo de servicios y de implementación de facilidades tecnológicas, los procesos de la entidad se adelantan con énfasis en la eficiencia, la transparencia y el control de la gestión y necesidades institucionales con las políticas operativas y de seguridad de la información, portafolio de proyectos y servicios, arquitectura de información y sistemas de información, plataforma tecnológica que posee la oficina de Informática para determinar las estrategias y apuntar a los dominios del marco de referencia.

7.1.1 Definición de los objetivos estratégicos de TI

• Integrar los sistemas de información de las diferentes Áreas de Distriseguridad que permitan la toma de decisiones sostenibles y eficientes.

• Incentivar la participación ciudadana y la innovación de la ciudad a través del empoderamiento y la confianza en el uso de TIC.

• Fortalecer la gestión de las tecnologías de la información y comunicaciones (TIC), que permita la adopción de los estándares y lineamientos de la arquitectura empresarial para un desarrollo incluyente, sostenido, participativo y transparente dentro de Distriseguridad.

• Habilitar las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de Distriseguridad y la eficiencia y transparencia del Estado.

• Implementar el sistema de gestión de servicio para gestionar de manera formalizada los requisitos del cliente, las demandas del negocio convirtiéndolas en servicios de TI, de acuerdo con la estrategia y el presupuesto.

• Incrementar la calidad y cantidad de los servicios en línea ofrecidos a los ciudadanos.

7.1.2 Alineación de la estrategia de TI con el plan

Dominios del marco de referencia de arquitectura de TI	Actividades	Producto	Plan Desarrollo
1. Estrategia de TI	1.1 Alineación de la estrategia de TI con la transformación institucional 1.2 Plan de seguridad y continuidad de la Información.	Estrategia de TI con la transformación institucional 1.2 Plan de seguridad y continuidad de la Información. Plan estratégico Integral de TI alineado con Plan de desarrollo de la organización y con arquitectura empresarial, en el que la gestión de TI represente un valor estratégico	Planes regionales de tecnologías de la información y las comunicaciones. Modernización institucional con transparencia y dignificación del servicio
2. Gobierno de TI	2.1 Crear y mantener una estructura organizacional que permita gestionar TI de manera integral y con valor estratégico. 2.2 Definición de procesos de gestión de TI. 2.3 Establecimiento de una arquitectura empresarial. 2.4 Sistema de Gestión integral de proyectos. (Lineamientos y estandarización de procesos para la planeación ejecución de los proyectos)	Oficina de TI consolidada y estructurada para desarrollar el plan estratégico con especialización técnica, empoderada con sostenibilidad técnica y financiera. Planes	Planes regionales de tecnologías de la información y las comunicaciones.
3. Gestión de información	3.1 Vista Integral del ciudadano. 3.2 Gestión documental para trámites y servicios en línea. (Repositorios de datos de Información)	Toda la información requerida por la entidad, el sector y otras entidades o instituciones, debe ser obtenida desde los sistemas de información, para atender las	Planes regionales de tecnologías de la información y las comunicaciones. Proyecto plataforma integradora

		necesidades de los actores interesados y empoderarnos para su uso efectivo en la toma de decisiones.	
4.Sistema de Información	4.1 Desarrollo y consolidación de los sistemas de información. 4.2 Gestión documental para trámites y Servicios en Línea. 4.3 Sistema Integrado de gestión financiera y cartera. 4.4 Sistema de Gestión integral de proyectos. (Sistema de información aplicativo)	Sistemas de Información que satisfagan las necesidades de los procesos y los servicios de la entidad y del sector.	Planes regionales de tecnologías de la información y las comunicaciones.
5.Gestión de Servicios Tecnológicos	5.1 Mantenimiento y adecuación de la conectividad interna y externa. 5.2 Implementación del sistema de gestión de servicios. 5.3 PMO y AE a nivel de ejecución de proyectos.	Internos y externos y que garantice la disponibilidad, seguridad y oportunidad de la tecnología de información que requiere la entidad.	Planes regionales de tecnologías de la información y las comunicaciones
6. Uso y apropiación de TI	6.1 Mantenimiento de la operación de los centros de apropiación. 6.2 Implementar y diseñar programas de TIC al ciudadano. 6.3 Promover el uso de los centros de apropiación mediante publicidad de cualquier tipo.	Desarrollar las herramientas y los mecanismos que hagan sostenible el uso y aprovechamiento de la tecnología y la información	Soluciones TIC al servicio del ciudadano implementadas Centros de apropiación (pvd, pvd+, vivelab) operando Ciudadanos capacitados en el uso de tecnologías de la información y la comunicación TIC

7.2 Gobierno de TI

7.2.1 Indicadores de gestión Informática

De acuerdo a la metodología referencial de IT4+, Distriseguridad se basa en los siguientes indicadores de gestión.

Nombre	Descripción
Nivel de ejecución del Plan de Estratégico de TI	Medirá el avance en la ejecución de los proyectos y actividades del plan
Base de datos con aseguramiento	Uso efectivo de los sistemas y servicios de información de Distriseguridad, en función de que las bases de datos cumplan los requisitos de conformidad que se desarrollan a través de los procesos de gestión de T.I.
Disponibilidad de información en medios de T.I.	Uso efectivo de los sistemas y servicios de información de la entidad
Nivel de requerimientos de desarrollo y mantenimientos implementados	Medir el avance en el desarrollo de los requerimientos y el mantenimiento de los sistemas de información con respecto a las necesidades de la arquitectura institucional.
Disponibilidad de las capacidades	Medir el nivel de operación para mantener el uso de los sistemas de información con base en la plataforma tecnológica.
Oportunidad en la solución a novedades de la plataforma tecnológica	Medir la oportunidad en la solución de novedades para mantener el uso de los sistemas de información con base en la plataforma tecnológica.

7.2.2 Riesgos Informáticos

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a Distriseguridad, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo.

Causas

- Desconocimiento y no aplicación de Políticas de Seguridad de la Información.
- Falta de análisis de vulnerabilidad/amenazas en los activos de información.
- Sacar a producción los sistemas de información sin haberlos probado anticipadamente.
- Intereses particulares por las personas encargadas de manipular el sistema.
- No contra con la infraestructura necesaria para el buen funcionamiento del sistema.
- Favorecimiento de intereses particulares.
- Insuficiencia en la asignación de recursos para los procesos informáticos.
- Vulnerabilidad en los prestadores de servicios externos.

Consecuencias de los riesgos no atendidos:

- Pérdida de credibilidad en la imagen institucional.
- Demandas Judiciales.
- Detrimento patrimonial.
- Pérdida de información.
- Retraso en los procesos.
- Gastos financieros.

Controles

- Política de seguridad de la información (POLÍTICA SGSI)
- Documentación de los mapas de riesgos de los proyectos
- Realización de pruebas y validación de vulnerabilidad
- Seleccionar personal idóneo para el desarrollo y manejo de los sistemas de Información.

Indicador o mecanismos de seguimiento

- Revisión controles de los riesgos en los comités de gestión de seguridad de la Información.
- Informes de supervisión y/o Productos.
- Auditorías a nivel de Gestión.

Los principales riesgos a tener en cuenta son:

1. Deficiente control de acceso a las aplicaciones: El acceso de los trabajadores a las aplicaciones debería estar mejor controlado.

2. Existencia de vulnerabilidades web: Accesos indebidos a información sensible de la Entidad.

3. Falta de formación y concienciación: La necesidad de potenciar la formación concienciación en materia de seguridad de la información al personal interno.

4. Proceso de gestión de incidentes de seguridad: La inexistencia o necesidad de mejora de la respuesta ante un incidente de seguridad.

5. Control de acceso a la red: Inexistencia de control de los accesos de los usuarios internos y terceros tales como proveedores o invitados a la red de Distriseguridad.

6. Fugas de información: La fuga de datos es uno de los mayores riesgos a los que se exponen las entidades.

7. Fraude y robo de información: Existe una gran vulnerabilidad en los llamados filtros informativos, lo que provoca que el fraude y robo de la información sea más común de lo que aparenta ser.

8. Uso de software seguro: aspectos clave en el ciclo de vida del uso de software.

7.2.3 Plan de implementación de procesos

El presente documento presenta los lineamientos a ejecutar en los años posteriores a su aprobación, se tiene como meta utilizar todas las metodologías y estrategias aquí planteadas para afianzar y alcanzar una administración con propósitos apoyados en un ambiente de TIC.

7.2.4 Estructura organizacional de TI

El esquema que se desea lograr es el siguiente:

7.3 Gestión de información

<table>
<tr><td rowspan="2"></td><td>PRINCIPIOS DE INFORMACION</td><td rowspan="2"></td></tr>
<tr><td>Diseñar los servicios de Información.</td></tr>
<tr><td rowspan="4">NECESIDADES DE INFORMACIÓN</td><td>Gestión de calidad de la Información.</td><td rowspan="4">SERVICIOS DE INFORMACIÓN</td></tr>
<tr><td>Gestión del ciclo de la Información.</td></tr>
<tr><td>Análisis de la información.</td></tr>
<tr><td>Desarrollo de capacidades para el uso estratégico de la Información.</td></tr>
</table>

Distriseguridad trabajará sobre los siguientes principios de Gestión de Información.

1. Información desde una Fuente: La construcción de fuentes "oficiales" de información debe constituirse como una de las políticas de calidad y dichas fuentes deben gozar de alta reputación, creíbles y que permitan ser mejoradas continuamente. Las fuentes únicas administran las categorías de datos principales en cada sector y se toman como elementos fundamentales de los flujos de datos. La definición de fuentes únicas de datos tiene como principal ventaja, mantener la coherencia del dato en el flujo de información, pero supone grandes retos de implementación que se resuelven a nivel de ingeniería de software, arquitectura de sistemas de información y de servicios tecnológicos.

2. Información de Calidad: En virtud que la información apoya la toma de decisiones a todo nivel, debe cumplir con los siguientes criterios: oportunidad, confiabilidad, completitud, pertinencia y utilidad. Se deben tener en cuenta, entre muchos otros aspectos, los lineamientos de política para el fortalecimiento de la calidad de la información que se emitan y adopten.

3. Información como Bien Público: El derecho a la información pública busca garantizar que esté disponible para todos los actores cuando la requieran, democratizar la información permite fortalecer la cultura del uso de la información y fomentar la toma de decisiones objetivas.

4. Información en Tiempo Real: Dado que los sistemas de información son representaciones de la realidad, disponer de la información con la inmediatez que se necesita, permite tener una representación más fiel de lo que está sucediendo en un momento particular, de tal forma que se puedan tomar decisiones y acciones (estratégicas y operativas) que tengan un mayor impacto.

5. Información pública como Servicio: La información pública es un servicio que los usuarios deberían consumir directamente de los sistemas de información al momento que lo necesitan con niveles de calidad satisfactorios.

7.3.1 Herramientas de análisis.

Algunas herramientas gratuitas Open-source para gestión de seguimiento, a las que habría que invertir en capacitación, ya que proporcionan información de importancia para la toma de decisiones.

7.3.2 Arquitectura de Información

Analizando la http://www.distriseguridad.gov.co principal objetivo es facilitar al máximo los procesos de comprensión y asimilación de la información que genera la entidad, así como las tareas que ejecutan los usuarios en los espacios de información y participación definidos.

La "arquitectura de la información" del sitio web de la entidad está basada en un proceso iterativo, transversal, que se dio a lo largo de todo el diseño del sitio y en cada una de sus fases, para asegurarse de que los objetivos de su producción y del desarrollo de la interfaz se cumplen de manera efectiva.

Permanentemente se busca impartir técnicas para ayudar al desarrollo y producción de espacios de información e interacción.

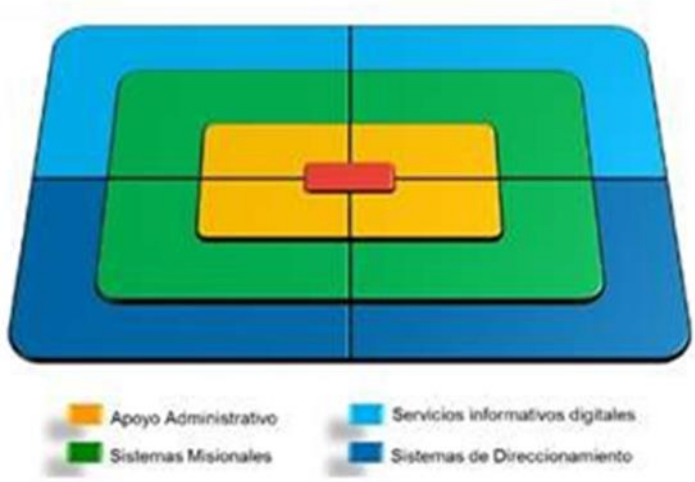
Con el fin de que la asimilación de contenidos por parte del usuario sea eficiente y efectiva, y para que el sitio sea accesible y usable, la Arquitectura de la Información del sitio web de la entidad, se encarga, durante el desarrollo, de definir:

- El objeto, propósito y fines del sistema de información o sitio.
- La definición del público objetivo y los estudios de la audiencia.

- La realización de análisis competitivos.
- El diseño de la interacción.
- El diseño de la navegación, esquemas de organización y facetación de los contenidos.
- El etiquetado o rotulado de los contenidos para acceder a la información.
- La planificación, gestión y desarrollo de contenidos.
- La facilidad de búsqueda y el diseño de la interfaz de búsqueda.
- La usabilidad.
- La accesibilidad.
- El fecedback del resultado y los procesos de "reingeniería" del sitio

Para aplicar el modelo conceptual de arquitectura de sistemas de información en Distriseguridad se debe seguir el siguiente proceso según IT4+:

Una vez recolectada la información sobre la existencia, administración y operación de los sistemas de información, y de la identificación de necesidades de comunicación de la organización se diseña la arquitectura de sistemas de información en la cual se pretende organizar los sistemas de acuerdo a su carácter: misional, apoyo, direccionamiento y de servicios de información, de tal manera que se garantice el flujo de información para la gestión, control y toma de decisiones.



En un primer nivel de la arquitectura se agrupan los sistemas de información de apoyo administrativo que constituyen el backoffice de la organización y usualmente contienen sistemas de planificación de recursos empresariales – ERP tales como (presupuesto, contabilidad, tesorería, caja, bancos, inventarios, activos fijos, entre otros), administración
de recursos humanos, gestión de infraestructura y gestión de tecnología. En este nivel se realizan las tareas operativas y repetitivas de tipo administrativo.

El segundo nivel es el de los sistemas misionales los cuales apoyan directamente la misión del negocio que desarrolla la organización. Estos sistemas dependen del tipo de misión que tenga la organización, por ejemplo, para los bomberos los sistemas misionales son los que apoyan la prestación del servicio.

El tercer nivel de la arquitectura de sistemas de información está formado por dos grandes mundos: uno de los servicios informativos digitales y otro de los sistemas de direccionamiento. Los servicios informativos digitales son todas aquellas herramientas que le permiten a los diferentes actores del sistema de información interactuar entre sí y con la información de los sistemas misionales y los de apoyo administrativo, desde una perspectiva de servicio y en un modelo organizado de portales de información.

Los sistemas de direccionamiento, por otra parte, son las facilidades que se le disponen a las instancias directivas y de decisión para hacer seguimiento oportuno a la ejecución de la estrategia definida, proporcionando información sobre el avance en el alcance de las metas e información para la toma de decisiones estratégicas.

La arquitectura de sistemas de información además implica que todos sus niveles y las piezas que componen cada nivel están lógica y adecuadamente interconectadas para permitir el flujo de información definido por los procesos de la organización.

Adicionalmente, propicia que el sistema de información cumpla con las principales premisas que hacen posible el análisis de la información: fuentes únicas de datos, información de calidad, información como servicio, información en tiempo real y la información como un bien público.

Dentro de cada nivel de la arquitectura se agrupan los sistemas o subsistemas de acuerdo con la categoría de información que soportan. Un sistema de información a su vez se compone de varios subsistemas o módulos con propósitos específicos.

7.4 Sistemas de información

Para apoyar los procesos misionales y de apoyo en una organización, es importante contar con sistemas de información que se conviertan en fuente única de datos útiles para la toma de decisiones en todos los aspectos; que garanticen la calidad de la información, dispongan recursos de consulta a los públicos de interés, permitan la generación de transacciones desde los procesos que generan la información y que sean fáciles de mantener. Que sean escalables, interoperables, seguros, funcionales y sostenibles, tanto en lo financiero como en lo técnico.

Bajo este esquema, Distriseguridad elabora los lineamientos tecnológicos en la implementación de sus sistemas de información.

Los sistemas de información que apoyan el sector operativo son:

- SIG
- Sigep 2
- Secop 2
- SAFE
- Tesorería bancos
- Pagina web
- Correo electrónico Outlook 365

En cuanto a la seguridad de los sistemas de información, se plantean los siguientes lineamientos:

El acceso a los sistemas de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

Los sistemas de información deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, los Discos externos y Servidores de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Google Drive) o en medios de almacenamiento alternos (Usb, Discos Externos).

Todos los sistemas de información que se tengan en operación deben contar con sus respectivos manuales actualizados.

Los sistemas de información deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).

Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad

7.4.1 Servicios de soporte técnico

El soporte técnico a los sistemas de información se planea de forma periódica para garantizar el máximo rendimiento y el mejor funcionamiento de los recursos de información y así mismo disminuir los factores de riesgo que amenazan permanentemente estos recursos.

7.5 Modelo de gestión de servicios tecnológicos

Distriseguridad se apoya en el modelo de gestión IT4+ para realizar el análisis de la gestión de los servicios de información.

Para disponer de los sistemas de información, es necesario desarrollar la estrategia de servicios tecnológicos que garantice su disponibilidad y operación con un enfoque orientado hacia la prestación de servicios que busque garantizar el uso de los sistemas de información mediante la implementación de un modelo de servicios integral que use tecnologías de información y comunicación de vanguardia, que contemple la operación continúa, soporte a los usuarios, la administración y el mantenimiento, y que implemente las mejores prácticas de gestión de tecnología reconocidas internacionalmente. Este modelo de servicios comprende el suministro y operación ininterrumpida (7x24x365) de la infraestructura tecnológica, almacenamiento, copias de seguridad (backup), datacenter, Web hosting dedicado, conectividad, seguridad física y lógica, monitoreo de infraestructura, mesa de ayuda y servicios de operación y mantenimiento entre los cuales se tienen: la administración de aplicaciones, administración de infraestructura de servidores, conectividad y seguridad.

El diagrama esquematiza los componentes que hacen parte del modelo de gestión de servicios tecnológicos dentro de los cuales se tienen: la infraestructura, la conectividad, los servicios de administración y operación, los servicios de soporte y mesa de ayuda, los procesos de gestión de servicios y los procesos de seguimiento e interventorías.

Adicionalmente, el esquema incluye: las relaciones del modelo con la estrategia y gobierno TI, toda vez que los servicios de tecnología deben desarrollarse en el marco de la estrategia de TI definida y teniendo en cuenta los esquemas de gobernabilidad establecidos para la gestión de TI; las áreas encargadas de sistemas de información y demás áreas involucradas en la prestación de los servicios, las cuales entregan los sistemas de información y aplicaciones que serán operadas por servicios tecnológicos; los proveedores de hardware, software y de telecomunicaciones que suministran los elementos y los servicios necesarios para garantizar la operación. Por último, se encuentran los beneficiarios o usuario finales de los servicios de TI ofrecidos por la organización.

7.5.1 Criterios de calidad y procesos de gestión de servicios de TIC

En el diseño de la arquitectura de servicios tecnológicos es necesario tener en cuenta los principios definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, para el dominio de servicios tecnológicos para la arquitectura empresarial del Estado colombiano y son los siguientes.

No	PRINCIPIO	DESCRIPCION
1	Capacidad	Este principio hace referencia a las previsiones sobre necesidades futuras basadas en tendencias, previsiones de negocio y acuerdos de niveles de servicios - ANS existentes, los cambios necesarios para adaptar la tecnología de TI a las novedades tecnológicas y a las necesidades emergentes de las entidades
2	Disponibilidad	Este principio es el responsable de optimizar y monitorizar los servicios TI para que estos funcionen ininterrumpidamente y de manera fiable, cumpliendo los ANS (Acuerdo de nivel de servicio).
3	Adaptabilidad	Las implementaciones tecnológicas deben ser adaptables a las necesidades de redefiniciones en las funciones de negocio de las entidades.
4	Cumplimiento de los	Toda institución del Estado cumplirá como mínimo con los estándares definidos por la arquitectura.
5	Oportunidad en la Prestación de	Permitir prestar un soporte técnico especializado de manera oportuna y efectiva.

7.5.2 Infraestructura

La modernización institucional con transparencia tiene como objetivo mejorar la eficiencia administrativa, prestar a los ciudadanos un servicio oportuno y de calidad, para ello se mejorará y aumentará la capacidad tecnológica actual entendida como un medio para lograr los fines propuestos.

Para ello se pretende mejorar y aumentar la capacidad tecnológica actual entendida como un medio para lograr los fines propuestos. Se tiene proyectado trabajar en la integración de los sistemas de información existentes, a través de una plataforma digital para centralizar y unificar la información que articule a todas las dependencias y entidades adscritas a la administración.

7.5.3 Conectividad

En cuanto a conectividad, Distriseguridad debe garantizar que:

Red local

Distriseguridad debe propender que La red área local debe estar diseñada para ofrecer los servicios de red de la entidad e interconectar la sede principal con todas las demás sedes de la administración. Estas deben ser redes de alta velocidad, con tecnología en fibra óptica y cableada que garanticen que los equipos se conecten a velocidades medidas en términos de gigabits por segundo. En un esquema de alta disponibilidad deben situarse canales de contingencia de similares características a los principales. La red puede estar segmentada según las necesidades de seguridad de la entidad. Para ello deben usarse dispositivos de seguridad que aíslen las redes o configuración de redes virtuales en los equipos activos de la red.

Red local inalámbrica

En Distriseguridad, la disposición de equipos es en su mayoría inalámbricos fijos y otros que habilitan la movilidad a los usuarios para conectarse a la red local y a Internet. Dependiendo del uso que se quiera ofrecer, habrá que dimensionar las redes inalámbricas para dar la cobertura y acceso en un 100% de las instalaciones de la entidad.
Dentro de estas redes se debe dimensionar el acceso con dispositivos móviles como celulares y/o tabletas, ya que estos disminuyen la capacidad de la red.
Vigilar las redes inalámbricas para funcionarios y visitantes garantizando la seguridad de la información de la entidad.

Internet

El ancho de banda instalado en la oficina de Distriseguridad es de 200 Mbps.
El servicio de Internet se dimensiona para ofrecer tráfico de salida y de entrada a Internet para toda la Administración y sus sedes. Dentro de los canales a contratar se diferencian las capacidades para canales de datos, canales de navegación y canales de publicación. En un esquema de alta disponibilidad se debería contar con un canal principal y un canal de backup, en lo posible en otro medio o con otro operador, de tal manera que se garantice la operación continua del servicio. Adicionalmente los canales cuentan con calidad del servicio o QoS (Quality of Service) y facilidades para administrar la priorización de los servicios.

7.5.4 Servicios de operación

Modelo de operación y administración de infraestructura tecnológica incluye todos los elementos de operación y servicios requeridos para garantizar la disponibilidad y operación de la plataforma tecnológica

7.5.5 Mesa de servicios

Se debe implementar La "mesa de servicio" es un conjunto de servicios con el objetivo de brindar soporte a los usuarios que lo requieran; La mesa de servicio se constituye en elemento vital del área de TI de la entidad, razón por la cual será el único contacto entre los funcionarios de planta, contratistas, organizaciones de soporte externas, servicios de TI y con el fin de canalizar todos las observaciones, reclamos, inquietudes, necesidades y cambios relacionados con TI en el día a día.

Debe estar constituida por un grupo de individuos con características especiales, para atender cualquier solicitud de servicio e incidencia, es de anotar que estas personas deben poseer idoneidad en este campo.
La mesa de servicio entregará informes de gestión, tomará contacto con los usuarios que lo requieran para atender sus llamadas o solicitudes de servicio y originará beneficios a toda la organización.

7.5.6 Procedimientos de gestión Estructura del Plan Estratégico de TI

La operación de los servicios tecnológicos de la entidad se debe realizar según los procedimientos de la cadena de valor de TI definida, los cuales se diseñaron teniendo en cuenta mejores prácticas internacionales de gestión de TI como ITIL, ISO/IEC 20000 y COBIT. La siguiente gráfica esquematiza el flujo entre los procedimientos de gestión de TI.

7.5.6.1 Gestión de niveles de servicio

Objetivo: definir, acordar, registrar y gestionar los niveles de servicio, garantizando su alineación con los servicios institucionales, para cumplir con los acuerdos establecidos.

Alcance: inicia con la disposición de la documentación de los servicios TIC ofrecidos, colaborando estrechamente con el cliente de acuerdo a sus necesidades, establecer los indicadores clave de rendimiento de los servicios de TIC y monitoreando la calidad de los servicios acordados; termina con la elaboración de informes sobre la calidad del servicio y los planes de mejora.

Las actividades principales que se llevan a cabo son las siguientes:

- Definir y ajustar el catálogo de servicios.
- Definir los requisitos del cliente.
- Planear los niveles de servicio.
- Negociar y documentar los Acuerdos de Niveles de Servicio - ANS.
- Monitorear y realizar seguimiento de los ANS.
- Mejorar el servicio.

7.5.6.2 Gestión de disponibilidad

Objetivo: asegurar que los servicios TIC estén activos cuando sean demandados, determinando los requisitos de disponibilidad en estrecha relación con acuerdos establecidos, con el objeto de proponer mejoras y aumentar los niveles de disponibilidad.

Alcance: inicia con la determinación de los requisitos de disponibilidad de los servicios TIC, desarrollo del plan de disponibilidad a corto y mediano plazo, diseño del mantenimiento del servicio en operación y recuperación de este en caso de fallo, elaboración de informes de seguimiento sobre disponibilidad y cumplimiento del servicio, hasta la evaluación del impacto de las políticas de disponibilidad de los servicios en la institución.

Las actividades principales que se llevan a cabo son las siguientes:

- Evaluar requisitos de la entidad.
- Planificar la disponibilidad.
- Gestionar interrupciones del servicio.
- Mantener / actualizar el plan.
- Monitorear.
- Comunicar niveles de disponibilidad.
- Proyecciones de mejora

7.5.6.3 Gestión de capacidad

Objetivo: determinar que los servicios TIC cumplen con las necesidades de capacidad tanto presentes como futuras, controlando su rendimiento y desarrollando planes de capacidad asociados a los niveles definidos, con el ánimo de gestionar y racionalizar la demanda de los servicios TIC.

Alcance: inicia desde la identificación del estado actual de los servicios TIC, los planes de negocio y acuerdos de nivel de servicio, análisis del rendimiento de la infraestructura para monitorear el uso de la capacidad existente, dimensionamiento adecuado de los servicios alineados con los procesos de la institución, hasta la gestión de la demanda de los servicios TIC.

7.5.6.4 Gestión de continuidad

Objetivo: garantizar la recuperación de los servicios de TIC en el evento de presentarse interrupciones. Se deben establecer políticas y procedimientos que eviten posibles consecuencias de fuerza mayor en el negocio, para ofrecer unos niveles aceptables de continuidad en el menor tiempo posible.

Alcance: inicia con el establecimiento de políticas de continuidad del servicio TIC, análisis de los impactos generados por la interrupción de los servicios TIC, análisis de los riesgos a los que están expuestos los servicios, adopción de medidas de prevención de riesgos en los servicios TIC, diseño, pruebas y revisión de planes de contingencias, hasta la formación del personal para la recuperación del servicio TIC.

Las actividades principales que se llevan a cabo son las siguientes:

- Planificación.
- Análisis del impacto del área de TI o BIA (Business Impact Analysis).
- Determinar estrategias de continuidad en el área de TI.
- Actualizar las Estrategias corporativas.
- Actualizar o diseñar la estrategia de nivel de actividad.
- Desarrollo e implantación de respuesta a la gestión de la continuidad del área de TI. Evaluación de conciencia y formación.
- Monitorización de los cambios culturales.
- Pruebas de los planes de acción.

7.5.6.5 Gestión de configuración

Objetivo: conservar un registro actualizado con el nivel de detalle de todos los elementos que integran la configuración de los servicios TIC, proporcionando información relevante de su conformación, para garantizar al máximo, el aprovechamiento de los elementos y apoyar efectivamente la gestión de cambios.

Alcance: inicia desde la planificación de los objetivos de la gestión de la configuración, la clasificación y registro del nivel de la configuración al detalle de los servicios TIC, monitoreo de los componentes autorizados en la configuración, y termina con la elaboración de informes de la configuración que sean requeridos.

Las actividades principales que se llevan a cabo son las siguientes:

- Realizar la planificación y gestión.
- Identificar la configuración.
- Toma de inventario / Línea base
- Clasificar los elementos de configuración - CI´s y descripción de estados de configuración.
- Determinar las relaciones entre CI´s y servicios.
- Actualizar la CMDB.
- Notificar la disponibilidad / Modificaciones de la CMDB.
- Verificar la CMDB.
- Hacer auditorías a la CMDB.
- Hacer auditorías y Verificación periódica.

7.5.6.6 Gestión de entrega

Objetivo: controlar la calidad de los servicios TIC, que se encuentran en producción, estableciendo políticas de nuevas versiones hechas a los servicios, después de las pruebas correspondientes, con el fin de garantizar que las entregas no afecten la calidad y actividad de los demás servicios en operación.

Alcance: El subproceso inicia con el establecimiento de una política para la generación e implementación de nuevas versiones de servicios TIC, retiro de servicios TIC que se encuentren en producción, actualización de registros de versiones de servicios TIC y termina con la comunicación formal a clientes y usuarios de la institución sobre las funcionalidades y beneficios de las nuevas versiones de servicios TIC.

Las actividades principales que se llevan a cabo son las siguientes:

- Entrega del RFC aprobado.
- Realizar la configuración inicial.
- Desarrollar el plan de liberación.
- Diseñar, construir y configurar la liberación.
- Diseñar el plan de back out.
- Convocar comité de aprobación.
- Preparar los ambientes
- Realizar pruebas de aceptación.
- Coordinar las liberaciones.
- Planificar capacitación.
- Capacitar.
- Distribuir/instalar la liberación.

- El requerimiento inicia nuevamente.
- Estabilización y pruebas en producción.
- Soporte oportuno o Early life support Ejecutar plan de back out.

7.5.6.7 Gestión de seguridad

Objetivo: mejoramiento continuo de una política de seguridad de la información, alineada con las necesidades de los clientes y usuarios, asegurando el cumplimiento de los estándares de seguridad, para que la información conserve la confidencialidad, la integridad y la disponibilidad.

Alcance: inicia desde la definición de la política de la seguridad de la información de los servicios TIC prestados a los clientes y usuarios, estándares de seguridad y confidencialidad firmados entre proveedores internos y externos, su monitoreo y evaluación, hasta la supervisión, análisis y tratamiento adecuados de riesgos, vulnerabilidades e impactos en los servicios TIC.

Las actividades principales que se llevan a cabo son las siguientes:

- Requisitos de seguridad.
- Identificación de riesgos.
- Planear.
- Comunicar e implementar.
- Evaluar.
- Mantener.

7.5.6.8 Gestión de cambios

Objetivo: administrar eficazmente los diferentes cambios que se presentan en los servicios TIC, garantizando el seguimiento de los procedimientos diseñados, con el fin de asegurar que los cambios se desarrollen en un entorno controlado minimizando el impacto que estos puedan tener en los servicios TIC.

Alcance: inicia desde el registro, evaluación y aceptación de los cambios en el servicio TIC; Desarrollo de la implementación de los cambios, aprobación de las solicitudes recibidas, la valoración de los resultados obtenidos y termina con la generación de informes de gestión y monitoreo de los cambios en los servicios TIC.

Las actividades principales que se llevan a cabo son las siguientes:

- Diligenciamiento y entrega del RFC.
- Validar información y completitud del RFC.

- Hacer registro y tipificación del RFC.
- Realizar evaluación del cambio.
- Implementar el cambio.
- Hacer revisión del cambio.
- Cerrar el registro del cambio.
- Informar al solicitante.

7.5.6.9 Gestión de incidentes

Objetivo: Restaurar los servicios tan rápido como sea posible, gestionando las interrupciones y degradaciones que se presenten en la prestación de los servicios TIC, para garantizar la prestación de los servicios según los acuerdos establecidos con los clientes

Alcance: inicia desde la clasificación y registro de incidentes presentados en la prestación de los servicios TIC, catalogar la criticidad según la prioridad dependiendo del impacto y la urgencia presentada, la asignación de los recursos y el personal necesario, monitoreo del estado y tiempos de respuestas a los incidentes, hasta la resolución y cierre de estos.

Las actividades principales que se llevan a cabo son las siguientes:

- Diseño de alto nivel.
- Identificación y registro del incidente.
- Búsqueda inicial de soluciones.
- Investigación y diagnóstico.
- Escalamiento si es necesario.
- Resolución y recuperación.
- Cierre de incidentes.
- Registro Web.
- Requerimientos.
- Administración de incidentes.
- Seguimiento y comunicación.

7.5.6.10 Gestión de problemas

Objetivo: identificar y eliminar la causa raíz de los incidentes recurrentes, determinando las posibles soluciones, que permitan garantizar los acuerdos de niveles de servicio.

Alcance: Inicia desde la clasificación y registro de los problemas para determinar sus causas y convertirlos en errores conocidos, identificación y registro en un repositorio de

soluciones y acciones preventivas y correctivas hasta la revisión post implementación de las soluciones.

Las actividades principales que se llevan a cabo son las siguientes:

- Identificar y registrar el problema.
- Categorizar y priorizar.
- Asignar recursos y programar tareas.
- Ejecutar técnica de diagnóstico.
- Recomendar solución.
- Cierre del problema.
- Reportes.
- Realizar seguimiento y comunicación.

7.5.6.11 Gestión de eventos

Objetivo: Detectar, clasificar y dimensionar los eventos que se presenten en los servicios TIC, a través del monitoreo de las alarmas definidas, para escalar los eventos, evitando interrupciones en la prestación de los servicios TIC.

Alcance: Inicia con el monitoreo y registro de los eventos y sucesos, continúa con el escalamiento de estos, hasta la generación de las bitácoras de eventos.

Las actividades principales que se llevan a cabo son las siguientes:

- Monitoreo de infraestructura.
- Detección de Eventos.
- Registro de Eventos.
- Exanimación y filtrado de eventos.
- Ejecutar acciones resolución del evento.
- Documentación y cierre de eventos.
- Administración del ciclo de vida de eventos.
- Reporte de eventos.

7.6 Uso y apropiación

componente de Uso y Apropiación de TI de Distriseguridad se apoya en el modelo de gestión IT4+ y debe ser una guía que provea a la entidad de herramientas y estrategias encaminadas a concientizar a funcionarios y usuarios sobre las oportunidades que presenta el uso de tecnologías de la información en su ámbito personal y profesional, mejorando su productividad y calidad de vida al hacer uso consciente de sistemas de información, dispositivos, herramientas de comunicación sincrónicas y asincrónicas,

buscadores Web, construcción de documentos en línea, herramientas para compartir o enviar archivos, acceso a la información, disponibilidad 24/7 y otros.

Entradas:

- Necesidades de Apropiación de los Componentes de TI Nuevas soluciones por implementar.
- Necesidades de los Procesos.
- Competencias individuales y grupales requeridas Planes de capacitación organizacionales y por áreas Restricciones y paradigmas vigentes.

Salidas:

- Incorporación del Cambio.
- Estrategia y acciones específicas de comunicación y divulgación
- Personas entrenadas con habilidades desarrolladas.
- Cambio incorporado en los procesos.
- Gestión de mejoramiento continúo en la adopción del cambio.
- Indicadores de uso.
- Herramientas de TI habilitadas para el gerenciamiento del cambio

8. MODELO DE PLANEACIÓN

8.1 Lineamientos y/o principios que rigen el plan estratégico de TIC: Los proyectos del presente documento PETI se alinean con la metodología IT4+ y el marco de referencia AE dado por Mintic.

1. Integración de Información: Se pretende en el ministerio hacer un mejor uso de la información que se tiene con los sistemas de información. Con un sistema de inteligencia de negocio el cual se divide en dos fases a nivel del ministerio y dos a niveles sectorial.

2. Trámites y Servicios al Ciudadano: Se busca mejorar los servicios que se prestan a la ciudadanía y con esto dar cumplimiento a GEL.

3. Datos Abiertos: Se desarrollará un plan para determinar qué datos se pueden abrir para dar un mejor aprovechamiento a estos y poder generar información útil a las demás entidades y a la ciudadanía.

4. Sellos de Excelencia: El Sello de Excelencia Gobierno en línea en Colombia es un instrumento que permite garantizar las condiciones de calidad necesarias para que el ciudadano acceda de manera confiable a los servicios digitales que ofrece el Estado colombiano. De esta manera, el Sello asegura que los ciudadanos cuenten con servicios digitales de muy alta calidad, ágiles, seguros, fáciles y efectivos.

Así mismo, y teniendo en cuenta lo dispuesto en el Decreto 1078 de 2015 en su artículo 2.2.9.1.4.3, el Sello está organizado bajo las siguientes categorías:

- Categoría servicios en línea: define los requisitos de calidad de los trámites y servicios en línea en cuanto a disponibilidad, seguridad, soporte, acceso, usabilidad, multicanalidad e interoperabilidad, de cara a la experiencia del usuario.

- Categoría gobierno abierto: establece los requisitos de calidad de los conjuntos de datos abiertos y plataformas de participación, que propicien un gobierno transparente, abierto y participativo.

- Categoría capacidades de Gestión de TI: establece las capacidades institucionales y operativas de las entidades públicas, que tienen como propósito asegurar el adecuado funcionamiento de sus recursos de TI.

5. Seguridad de la Información: Se dará continuidad a la política de SGSI construida y se mantendrá el fortalecimiento de la seguridad de la información, esperando lograr la certificación en este tema para el 2023.

6. Interoperabilidad: Se realizará un proyecto de interoperabilidad con el sector público

7. Activos de Información: Se trabajará en el desarrollo de un aplicativo automatizado que permita una fácil recolección de datos para inventariar los activos de información.

9. Caracterización de Usuarios: Se trabajará en optimización del portal de PQRS de la pagina web de la entidad para que permita una fácil recolección de datos característicos de la ciudadanía, al momento de solicitar servicios o trámites en Distriseguridad.

Ítem	Proyecto	Fecha Ejecución	Presupuesto	Responsable de Ejecución
1	Actualización de equipos de computo (Cambio de discos duros y memorias)	Febrero -23	$6.000.000	Ingeniero Tic
2	Adquisición de servidor local (cloud y físico)	Marzo -23	$28.000.000	Ingeniero Tic
3	Software antivirus	Abril - 2023	10.000.000	Ingeniero Tic
4	Proyecto de implementación de ups y reestructuración de cableado eléctrico.	Mayo - 2023	$28.000.000	Ingeniero Tic
5	Adquisición de cámaras de seguridad y alarma contraincendios	Mayo - 2023	$22.000.000	Ingeniero Tic
6	Proyecto de restructuración de datos con cableado estructurado (voz y datos) y cambio de direccionamiento ip v4 a ip v6	Agosto	$28.000.000	Supervisor Tic
7	Licencias Microsoft 365	Noviembre	20.000.000	Ingeniero Tic

ENRIQUE BRIEVA JURADO
PUE Planeación
Coordinador grupo de Trabajo TIC`s
Secretario técnico MIPG

Elaborado por: Ing. Victor Santiz P.
Fecha de elaboración: 20/01/2023