Secretaría de Planeación

MIPG

Modelo Integrado de Planeación y Gestión

Septiembre 2020

POLITICA 6: GOBIERNO DIGITAL
POLITICA 7: SEGURIDAD DIGITAL

D03: GESTIÓN PARA RESULTADOS CON VALORES

Septiembre 2020

CONTENIDO

1. Generalidades Dimensión 03

P06: Gobierno Digital

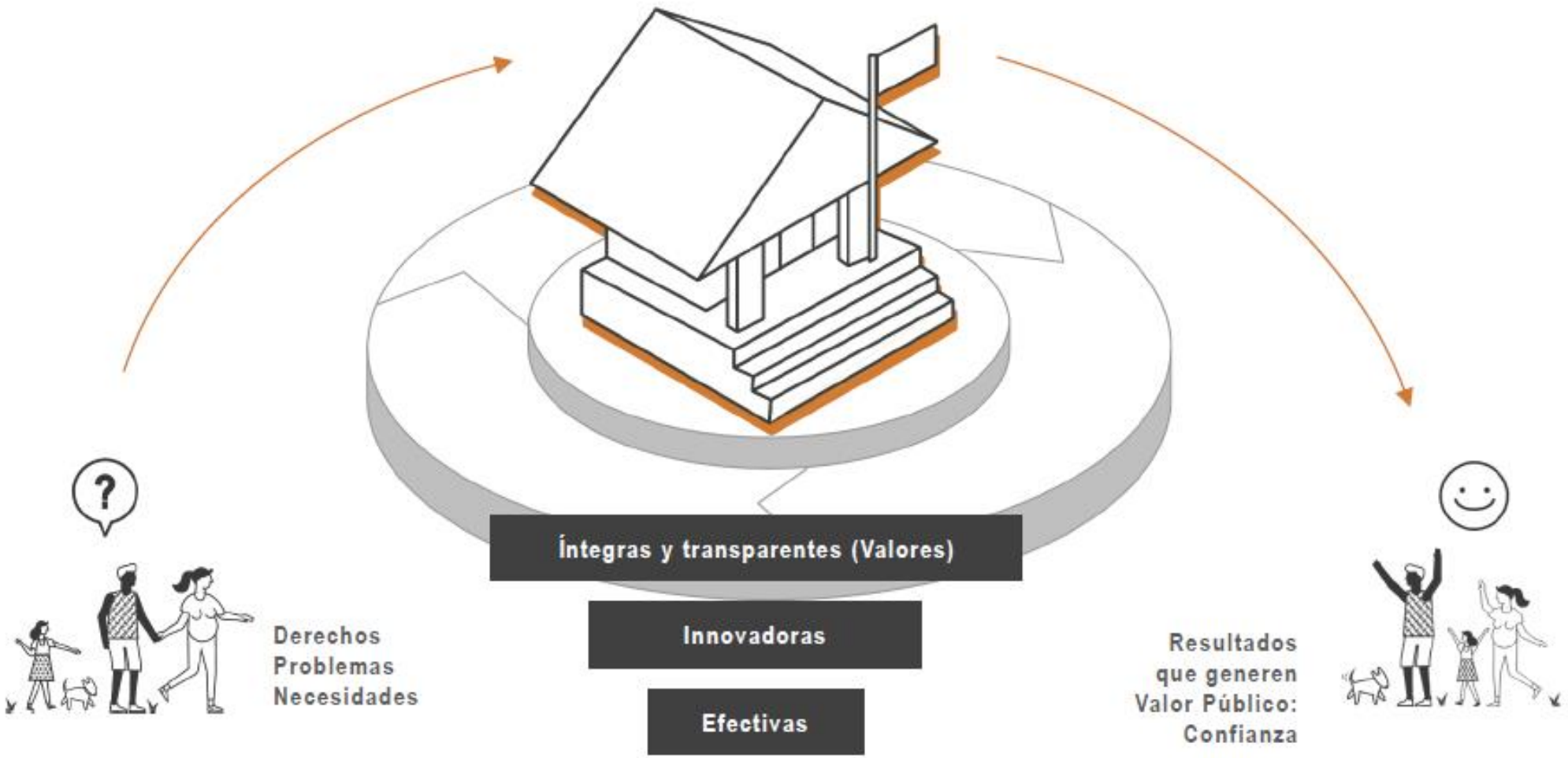
P07: Seguridad Digital

2. Resultados FURAG

3. Recomendaciones y Plan de Acción

4. Preguntas

Todos soñamos con Entidades Públicas



Gestión de las Entidades Públicas

Recursos presupuestales, físicos y tecnológicos

Talento humano

Planear, ejecutar contratar

Controlar, prevenir, documentar, promover buen servicio, gestionar conocimiento

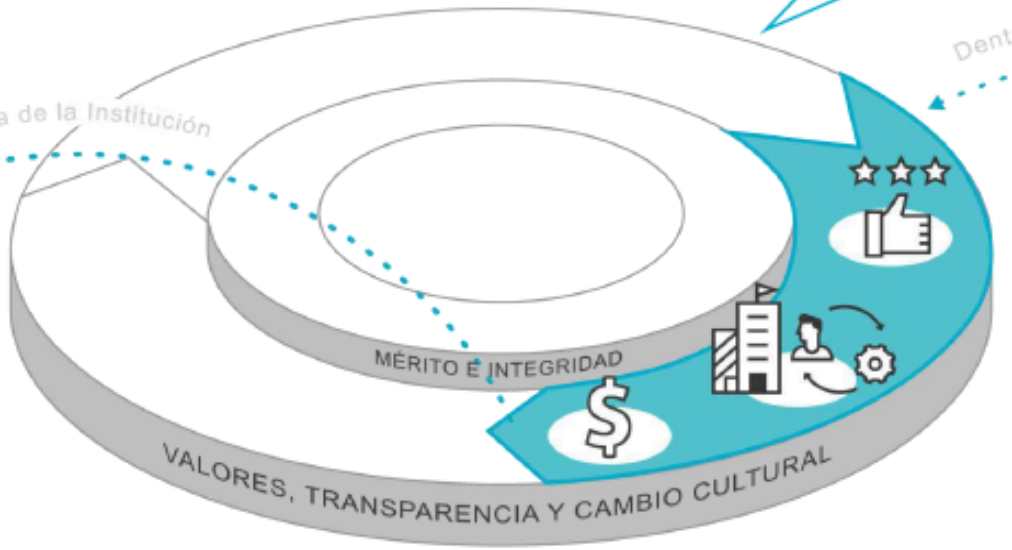
Evaluar, rendir cuentas, suministrar información, promover transparencia y comunicar

2. GESTIÓN PARA RESULTADOS CON VALORES

DIMENSIÓN 3

Gestión con Valores para resultados

La Dimensión de gestión con valores para resultados será abordada desde dos enfoques, en primer lugar de la ventanilla hacia adentro donde se concentran mayor parte de las políticas y relación estado ciudadano



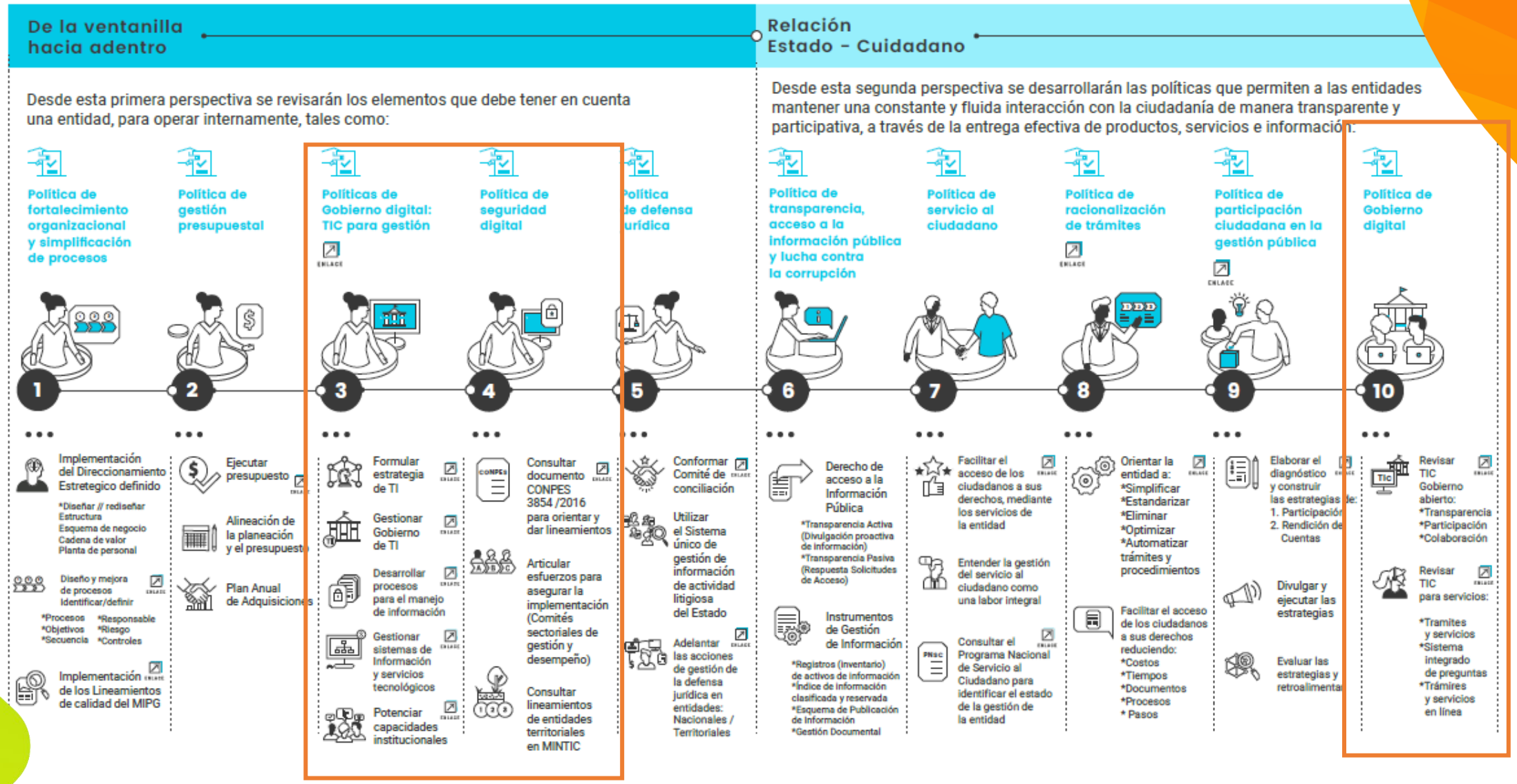
RELACIÓN ESTADO – CIUDADANO

- Racionalización de Trámites
- Participación ciudadana en la gestión pública
- Servicio al Ciudadano
- Gobierno Digital

DE LA VENTANILLA HACIA ADENTRO

- Fortalecimiento organizacional y simplificación de procesos
- Gestión Presupuestal y eficiencia del Gasto público
- Gobierno digital
- Seguridad digital
- Defensa jurídica
- Mejora normativa

2. GESTIÓN PARA RESULTADOS CON VALORES



POLITICA DE GOBIERNO DIGITAL

Esta política busca fortalecer la relación estado sociedad e incorporar el uso de las TIC en la operación de la entidad, así como:

1. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
2. Tomar decisiones basadas en datos, a partir del aumento del uso y aprovechamiento de la información.
3. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.
4. Impulsar el desarrollo de territorios y ciudades inteligentes, para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.
5. Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad

OBJETIVO

Uso y aprovechamiento de las TIC para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital

	ESTADO	SOCIEDAD
	IDÓNEAS, PREPARADAS Y CON ALTA CALIDAD EN SUS PROCESOS Y LA IMPLEMENTACIÓN DE POLÍTICAS	TIENEN CAPACIDADES Y RECURSOS SENCILLOS Y EFECTIVOS PARA INTERACTUAR CON EL ESTADO A TRAVÉS DE LOS MEDIOS DIGITALES
	ANTICIPAN, PREVISIVAS, MITIGAN RIESGOS, Y CONOCEN AVANCES TECNOLÓGICOS QUE IMPLEMENTAN DE ACUERDO A SUS NECESIDADES	PARTICIPAN EN EL DISEÑO DE TRÁMITES Y SERVICIOS; POLÍTICAS; NORMAS; PROYECTOS Y EN LA TOMA DE DECISIONES POR MEDIOS DIGITALES
	PROMUEVEN/INCENTIVAN LA INTERACCIÓN Y COLABORACIÓN ENTRE DIFERENTES ACTORES PARA LA GENERACIÓN DE VALOR PÚBLICO USANDO MEDIOS DIGITALES	AYUDAN A IDENTIFICAR Y RESOLVER PROBLEMÁTICAS Y NECESIDADES COMUNES; PARTICIPAN EN ESPACIOS DE ENCUENTRO Y COLABORACIÓN CON DIFERENTES ACTORES

DEFINICIÓN DE VALOR PÚBLICO Y CONFIANZA DIGITAL

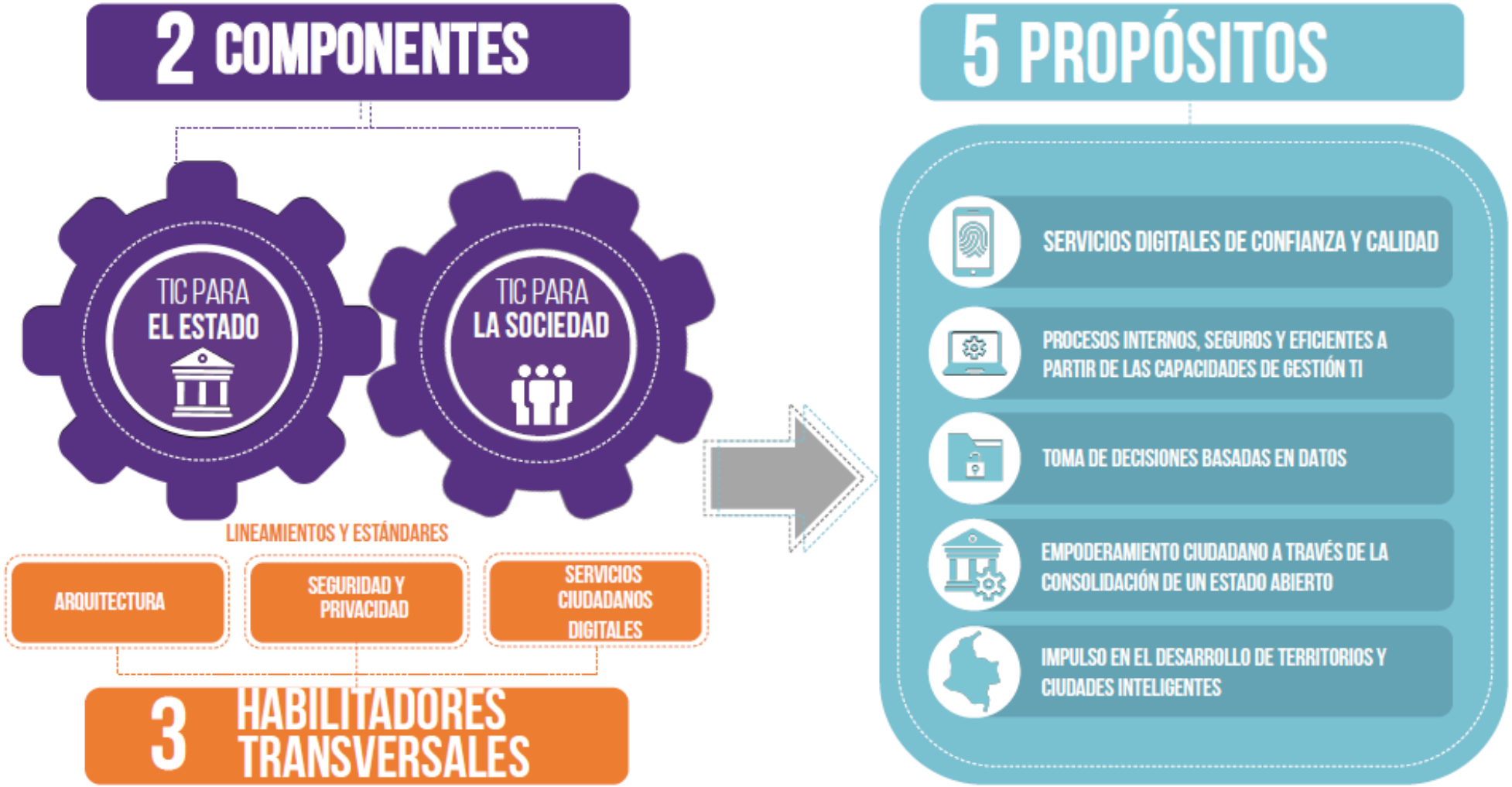
VALOR PÚBLICO

- GARANTÍA DE DERECHOS, SATISFACCIÓN DE NECESIDADES Y PRESTACIÓN DE SERVICIOS DE CALIDAD
- ESTADO QUE LLEGA A DONDE NO LLEGA EL MERCADO Y CREACIÓN DE NUEVOS MERCADOS
- GOBERNANZA DESDE LA PARTICIPACIÓN Y LA LEGITIMIDAD

CONFIANZA DIGITAL

- ESTADO, OFERTA INSTITUCIONAL Y ACCIÓN CIUDADANA EN UN AMBIENTE DIGITAL CORRESPONSABLE, PREVISIBLE Y SEGURO
- DIÁLOGO PERMANENTE ENTRE LOS ACTORES DEL ECOSISTEMA DIGITAL
- MEDIOS DIGITALES ÁGILES, SENCILLOS Y ÚTILES

ESTRUCTURA


2 COMPONENTES
TIC PARA EL ESTADO
TIC PARA LA SOCIEDAD
LINEAMIENTOS Y ESTÁNDARES
ARQUITECTURA
SEGURIDAD Y PRIVACIDAD
SERVICIOS CIUDADANOS DIGITALES
3 HABILITADORES TRANSVERSALES
5 PROPÓSITOS
SERVICIOS DIGITALES DE CONFIANZA Y CALIDAD
PROCESOS INTERNOS, SEGUROS Y EFICIENTES A PARTIR DE LAS CAPACIDADES DE GESTIÓN TI
TOMA DE DECISIONES BASADAS EN DATOS
EMPODERAMIENTO CIUDADANO A TRAVÉS DE LA CONSOLIDACIÓN DE UN ESTADO ABIERTO
IMPULSO EN EL DESARROLLO DE TERRITORIOS Y CIUDADES INTELIGENTES

INSTITUCIONALIDAD

Componente TIC para el Estado

Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con las demás entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.

A través de este componente, se busca que las entidades fortalezcan:

- Competencias de tecnologías de la información -T.I.
- Arquitectura institucional
- Competencias de sus servidores públicos

como elementos generadores de valor en la gestión pública.

Componente TIC para la Sociedad

Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común

A través de este componente se busca mejorar :

Conocimiento, uso y aprovechamiento de las TIC, por parte de los usuarios, ciudadanos y grupos de interés

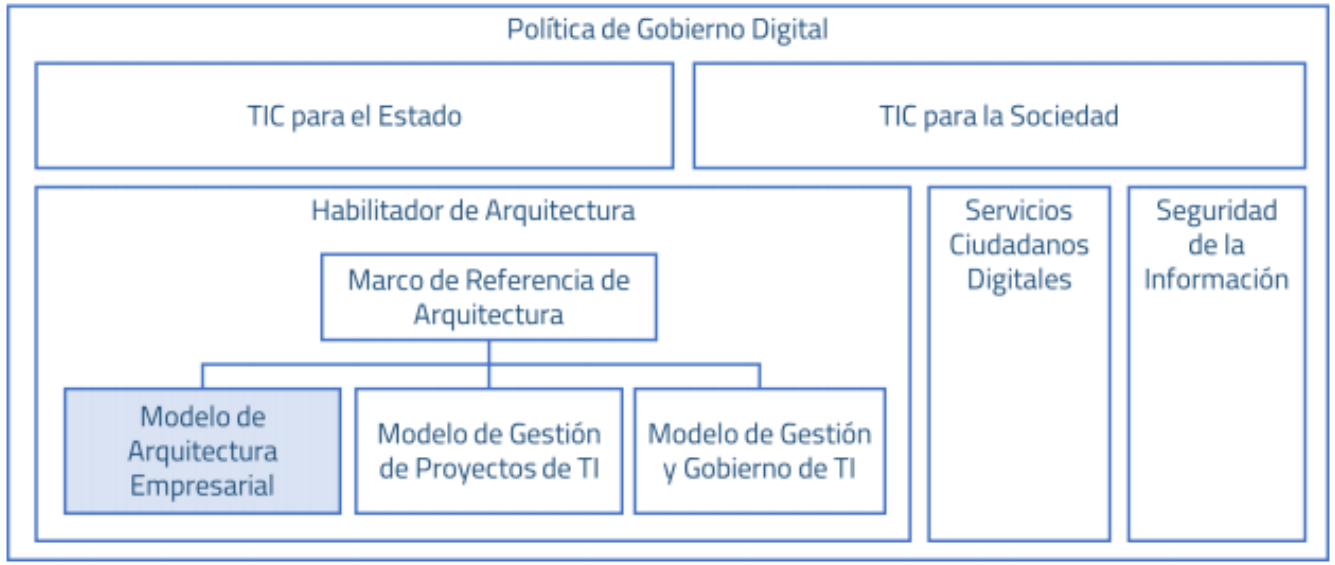
Acceso a la información pública, a trámites y servicios

Participación en la gestión pública y en la satisfacción de necesidades.

1

Habilitador Transversal de Arquitectura

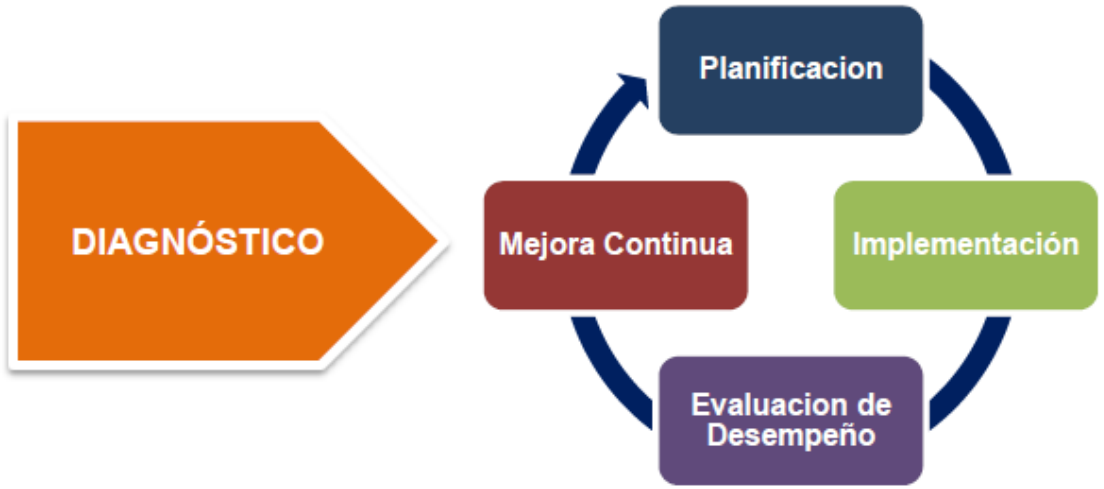
Busca que las entidades públicas apliquen en su gestión, un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI, aplicando los lineamientos, estándares y mejores prácticas contenidos en el Marco de Referencia de Arquitectura Empresarial del Estado.



2

Habilitador de Seguridad de la Información

Busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.



3

Habilitador de Servicios Ciudadanos Digitales

Busca que los servicios ciudadanos digitales sean integrados a los procesos, servicios digitales, trámites digitales, sistemas de información y demás que lo requieran, buscando racionalizar recursos, estandarizar y armonizar la administración pública en pro de mejorar los servicios del Estado.

servicios básicos

- autenticación electrónica, carpeta ciudadana e interoperabilidad

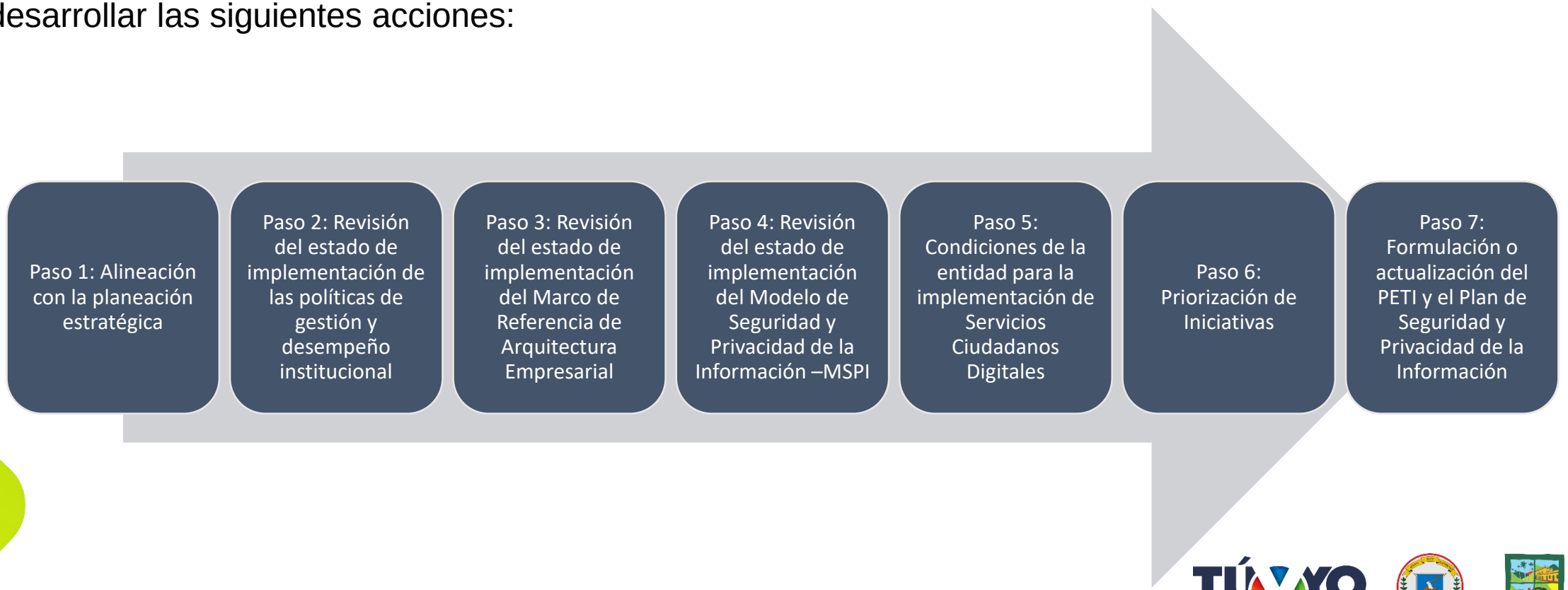
Servicios adicionales

- desarrollo de aplicaciones o soluciones informáticas para la prestación de los servicios ciudadanos digitales básicos

Planear la política de Gobierno Digital

Las acciones orientadas a planear la política de Gobierno Digital en cada entidad deben estar estrechamente relacionadas con la Planeación Estratégica de la entidad y las políticas de gestión y desempeño institucional.

En este sentido, la política de Gobierno Digital es un eje que permite impulsar el desarrollo de la gestión de la entidad. Por ello, para planear política de Gobierno Digital, se requiere desarrollar las siguientes acciones:



Paso 1: Alineación con la planeación estratégica

Identifique en el plan de acción, plan estratégico o plan de desarrollo departamental, los proyectos o iniciativas que aportan al logro de los propósitos de la política de Gobierno Digital **o que para su desarrollo incorporan el uso de las TIC**

Elabore un listado para priorizarlos en términos de tiempos, recursos y costos

Priorice proyectos o iniciativas en materia de salud, educación, empleo, transporte, cultura, medio ambiente, fortalecimiento organizacional, teletrabajo, proyectos orientados al logro de los Objetivos de Desarrollo Sostenible, proyectos de innovación con uso de TIC, proyectos de ciudades inteligentes, implementación del mapa de ruta de Gobierno Digital o la **solución a retos y problemáticas pública**

Paso 2: Revisión del estado de implementación de las políticas de gestión y desempeño institucional

Revise la implementación de las políticas de gestión y desempeño institucional en la entidad e **identifique cómo el uso de tecnologías puede impulsar el desarrollo de tales políticas.**

- Planeación Institucional
- Talento humano
- Transparencia, acceso a la información pública y lucha contra la corrupción
- Fortalecimiento organizacional y simplificación de procesos
- Servicio al ciudadano
- Participación ciudadana en la gestión pública
- Racionalización de trámites
- Gestión documental
- Seguridad Digital
- Gestión del conocimiento y la innovación

listado de proyectos o iniciativas que hacen uso de TIC para apoyar el desarrollo de una o varias de estas políticas

Paso 3: Revisión del estado de implementación del Marco de Referencia de Arquitectura Empresarial

identifique el estado de avance del Marco de Referencia de Arquitectura Empresarial

Aplique el formato de autodiagnóstico de MIPG

A partir de los resultados obtenidos, defina actividades, proyectos o iniciativas para continuar con la implementación del Marco

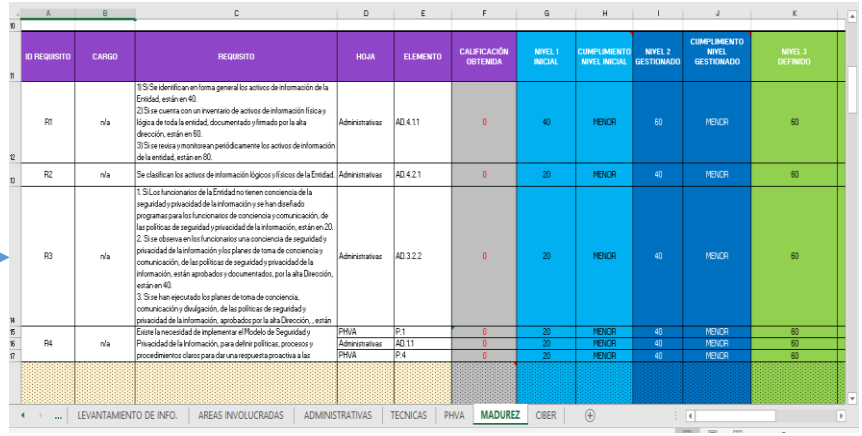
Disponibilidad de recursos, responsables, tiempos de ejecución y productos concretos a entregar en la vigencia por parte de la entidad

Departamento del Quindío

Paso 4: Revisión del estado de implementación del Modelo de Seguridad y Privacidad de la Información -MSPI:

Aplique el formato de autodiagnóstico de MIPG

instrumento de evaluación del MSPI disponible en el sitio web de Modelo



A partir de los resultados obtenido, defina actividades, proyectos o iniciativas para continuar con la implementación del Modelo,

Disponibilidad de recursos, responsables, tiempos de ejecución y productos concretos a entregar en la vigencia por parte de la entidad

Departamento del Quindío

Paso 5: Condiciones de la entidad para la implementación de Servicios Ciudadanos Digitales:

Son soluciones tecnológicas que buscan optimizar la labor del Estado y facilitar a los ciudadanos su interacción con la administración pública.

Son el conjunto de herramientas y procesos (Interoperabilidad, Carpeta Ciudadana y Autenticación Digital) que le permiten al ciudadano acceder de manera eficiente a los servicios y trámites del Estado a través de medios electrónicos.

Servicio de interoperabilidad

- Es el servicio que brinda las capacidades necesarias para garantizar el adecuado flujo de información e interacción entre los sistemas de información de las entidades, permitiendo el intercambio, la integración y la compartición de la información, con el propósito de facilitar el ejercicio de sus funciones constitucionales y legales, acorde con los lineamientos del marco de interoperabilidad.

Servicio de Autenticación Electrónica

- Es el procedimiento que, utilizando mecanismos de autenticación, permite verificar los atributos digitales de una persona cuando adelanta trámites y servicios a través de medios digitales. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que se atribuya el mismo.

Servicio de Carpeta Ciudadana

- Es el servicio que le permite a los usuarios de servicios ciudadanos digitales acceder digitalmente de manera segura, confiable y actualizada al conjunto de sus datos, que tienen o custodian las entidades públicas o particulares que ejercen funciones administrativas. Adicionalmente, este servicio podrá entregar las comunicaciones o alertas que las entidades señaladas tienen para los usuarios, previa autorización de estos.

Dichos servicios ciudadanos básicos ciudadanos serán provistos por operadores y articulados por la [Agencia Nacional Digital]

¿Quiénes intervienen en los Servicios Ciudadanos Digitales?

Usuarios

Ciudadano colombiano o extranjero, entidades públicas o privadas que requieran solicitar un servicio o trámite ante el estado.

Articulador

Entidad pública definida por el Ministerio TIC que garantiza el funcionamiento de las herramientas y procesos que permiten prestar los SCD.

Prestador de SCD

Entidad pública y/o privada que provee los SCD de Carpeta Ciudadana, Interoperabilidad, Autenticación Digital a los usuarios bajo los lineamientos expedidos por Mintic.

1

- Identifique la situación de la entidad frente a la implementación del decreto 1413 de 2017 sobre servicios ciudadanos digitales

2

- Priorice o establezca un plan de acción para la implementación de este decreto.

3

- Tenga en cuenta la gradualidad de la implementación establecida en el artículo 2.2.17.8.1 del DUR-TIC
- Los lineamientos definidos en el anexo No. 4 del Manual de Gobierno Digital

Paso 6: Priorización de Iniciativas

a partir de los proyectos, iniciativas y acciones identificados en los pasos 1, 2, 3, 4 y 5

- establezca un orden de ejecución de acuerdo a las metas, tiempos y recursos de la entidad

llévelos al Plan Estratégico de Tecnología – PETI y al Plan de Seguridad de la Información,

identifique cómo cada uno de los proyectos apuntan al cumplimiento de los propósitos de la política de Gobierno Digital,

Proyectos o iniciativas que buscan brindar servicios ágiles, sencillos y útiles para usuarios y grupos de interés a través de las TIC

Proyectos o iniciativas de mejoras en procesos y procedimientos que usan las TIC, implementación o mejoras a sistemas de información, servicios tecnológicos o fortalecimiento del talento humano para el aprovechamiento de las TIC

Proyectos o iniciativas que impulsan el desarrollo de servicios, políticas, normas, planes, programas, proyectos o asuntos de interés público, a través del uso de datos que cuentan con estándares de calidad y seguridad

Proyectos o iniciativas que buscan involucrar a ciudadanos, usuarios y grupos de interés de la entidad en el diseño y ejecución de servicios, políticas, normas y en la solución de necesidades o problemáticas públicas, a través de las TIC

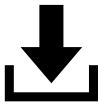
Proyectos o iniciativas de tipo social, ambiental, político o económico, que buscan impulsar el desarrollo sostenible o mejorar la calidad de vida de ciudadanos, usuarios o grupos de interés, haciendo uso de las TIC

Plan Estratégico de Tecnologías –PETI

El Plan Estratégico de las Tecnologías de la Información y Comunicaciones es el artefacto que se utiliza para expresar la Estrategia de TI.

Incluye una visión, unos principios, unos indicadores, un mapa de ruta, un plan de comunicación y una descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos, etc.) necesarios para la puesta en marcha y gestión del plan estratégico.

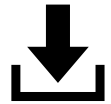
El PETI hace parte integral de la estrategia de la institución. Cada vez que una entidad hace un ejercicio o proyecto de Arquitectura Empresarial, su resultado debe ser integrado al PETI.



Plan de Seguridad y Privacidad de la Información

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la entidad, con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

En el plan de seguridad se establecen los detalles de cómo se realizará la implementación de la seguridad de la información en cada uno de los procesos de la entidad, estipulando directrices, tiempo y responsables para lograr un adecuado proceso de gestión, administración y evaluación de esta.



Ejecutar la política de Gobierno Digital

Lineamientos TIC para el Estado y TIC para la Sociedad

Asegure la generación de valor para la entidad y los usuarios "Use la tecnología para resolver necesidades y no por que debe cumplir"	•Identifique el problema o necesidad y los actores relacionados con el proyecto •Identifique y analice información y datos proactivamente •Evalúe la aplicación de metodologías de innovación •Aplique directrices de inversión inteligente
Cuente con la participación de todos "Aplique el valor de trabajar en equipo"	•Asegure el respaldo de la alta dirección •Genere integración y colaboración entre todas las áreas responsables •Busque colaboración con otras entidades •Cuente con equipos multidisciplinarios •Establezca alianzas entre diferentes actores
Diseñe integralmente su proyecto "Trabaje con los beneficiarios y piense en todos los detalles"	•Estructure todo proyecto con un enfoque de arquitectura empresarial •Involucre a los usuarios en el diseño y ejecución del proyecto •Garantice que el proyecto sea ambientalmente sostenible •Incorpore los principios de diseño de servicios digitales
Gestione el proyecto de principio a fin " Garantice buenos resultados y satisfacción de necesidades"	•Defina y ejecute el ciclo de gestión del proyecto •Gestione la información como un producto o servicio de calidad •Desarrolle un esquema de seguimiento y evaluación •Desarrolle acciones de mejora continua •Estrategia de gestión de conocimiento, uso y apropiación

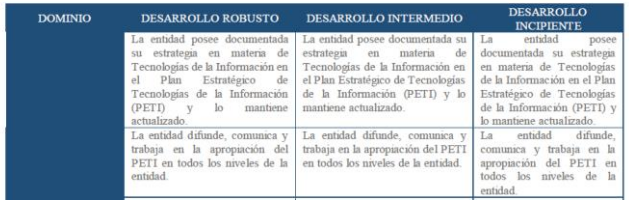
Lineamientos de los elementos habilitadores

Entidades Territoriales: se clasifican en entornos de desarrollo robusto, intermedio e incipiente, a partir de la identificación de características propias de cada municipio y departamento en relación con seis temáticas que precisan las condiciones territoriales.

Grupos de entidades para el nivel nacional	Entorno de desarrollo para la implementación de Gobierno Digital
1 y 2	Entorno de desarrollo robusto
3 y 4	Entorno de desarrollo intermedio
5 y 6	Entorno de desarrollo incipiente

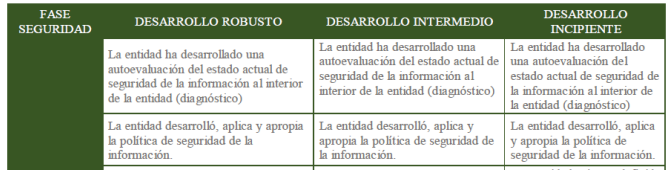
A partir de la clasificación anterior, los elementos habilitadores de Arquitectura y Seguridad de la Información fueron adaptados a cada entorno de desarrollo, de forma que la entidad deberá implementarlos de acuerdo con su clasificación.

5.2. Anexo 2 - Segmentación Elementos Habilitadores: Arquitectura



DOMINIO	DESARROLLO ROBUSTO	DESARROLLO INTERMEDIO	DESARROLLO INCIPIENTE
	La entidad posee documentada su estrategia en materia de Tecnologías de la Información en el Plan Estratégico de Tecnologías de la Información (PETI) y lo mantiene actualizado.	La entidad posee documentada su estrategia en materia de Tecnologías de la Información en el Plan Estratégico de Tecnologías de la Información (PETI) y lo mantiene actualizado.	La entidad posee documentada su estrategia en materia de Tecnologías de la Información en el Plan Estratégico de Tecnologías de la Información (PETI) y lo mantiene actualizado.
	La entidad difunde, comunica y trabaja en la apropiación del PETI en todos los niveles de la entidad.	La entidad difunde, comunica y trabaja en la apropiación del PETI en todos los niveles de la entidad.	La entidad difunde, comunica y trabaja en la apropiación del PETI en todos los niveles de la entidad.

5.3. Anexo 3 - Segmentación Elementos Habilitadores: Seguridad de la Información



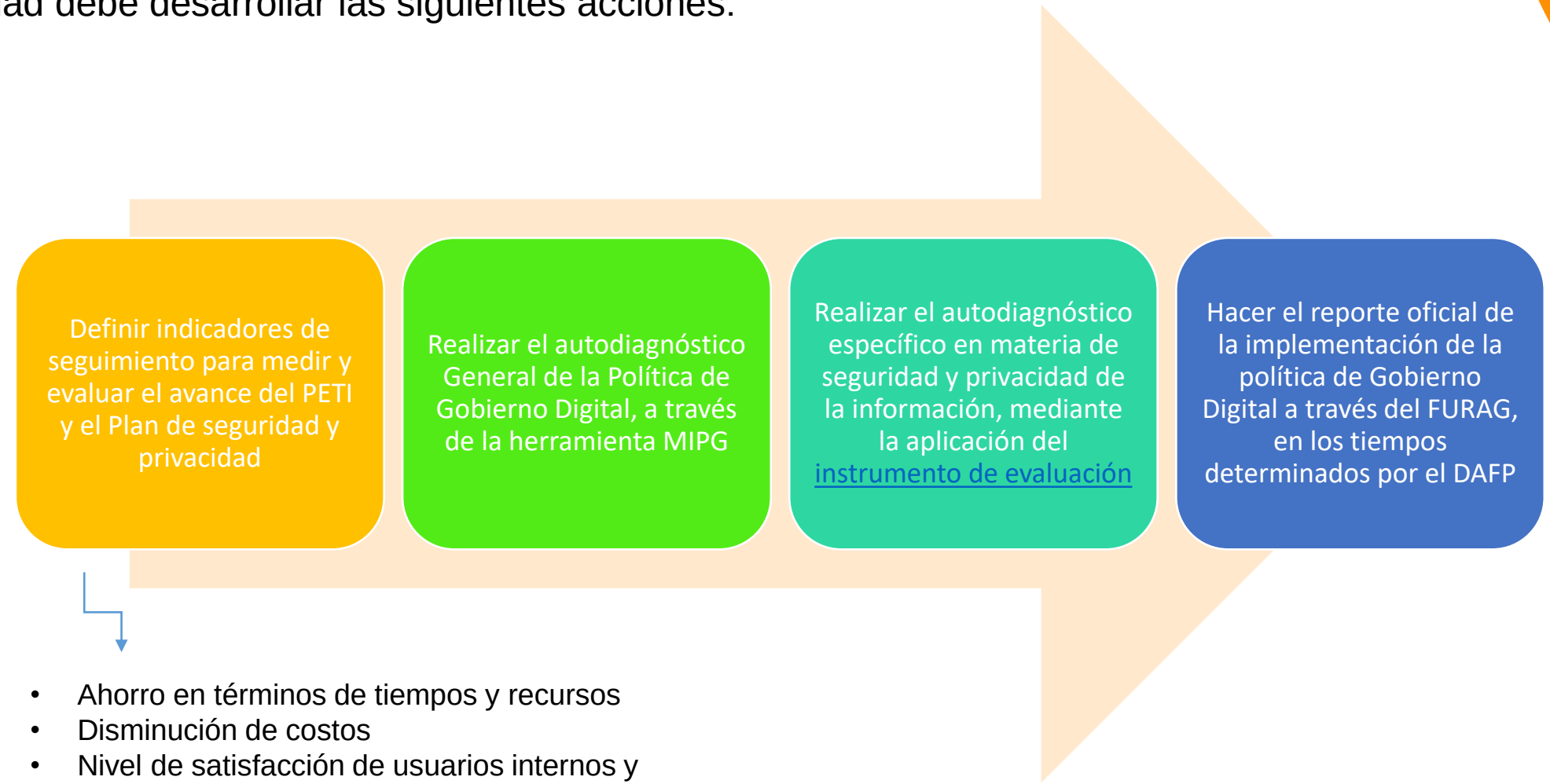
FASE SEGURIDAD	DESARROLLO ROBUSTO	DESARROLLO INTERMEDIO	DESARROLLO INCIPIENTE
	La entidad ha desarrollado una autoevaluación del estado actual de seguridad de la información al interior de la entidad (diagnóstico)	La entidad ha desarrollado una autoevaluación del estado actual de seguridad de la información al interior de la entidad (diagnóstico)	La entidad ha desarrollado una autoevaluación del estado actual de seguridad de la información al interior de la entidad (diagnóstico)
	La entidad desarrolló, aplica y apropia la política de seguridad de la información.	La entidad desarrolló, aplica y apropia la política de seguridad de la información.	La entidad desarrolló, aplica y apropia la política de seguridad de la información.

En relación con el elemento habilitador de Servicios Ciudadanos Digitales, se han diseñado lineamientos específicos que deben ser implementados por todas las entidades en cumplimiento de lo dispuesto en el título 17, parte 2, libro 2 del Decreto 1078 de 2015,

Medir la política de Gobierno Digital

a. Seguimiento y Evaluación por parte de la Entidad

La entidad debe desarrollar las siguientes acciones:



- Ahorro en términos de tiempos y recursos
- Disminución de costos
- Nivel de satisfacción de usuarios internos y externos
- Tasas de uso de procesos, trámites y servicios digitales vs. Presenciales

b. Seguimiento y Evaluación por parte del MinTIC

Verificará que cada sujeto obligado presente resultados anuales mejores que la vigencia anterior. Para ello, se aplicarán indicadores de cumplimiento e indicadores de resultado, de acuerdo con los criterios de evaluación y seguimiento definidos por el Consejo para la Gestión y Desempeño institucional

Así mismo, se realizarán mediciones de calidad a través del Sello de Excelencia de Gobierno Digital.

Indicadores de Resultado: buscan medir el cumplimiento de los logros de la política de Gobierno Digital y son los siguientes:

1.Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad	
% de trámites, servicios y OPAs digitales con sello de excelencia	Tasa de completitud del trámite, servicio y OPAs digital

2.Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información	
% de procesos y procedimientos internos con sello de excelencia	% de procesos y procedimientos que optimizaron tiempos de ejecución y son más sencillos

3.Tomar decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la información		
% de datos abiertos certificados con sello de excelencia	% de datos abiertos de la entidad que están siendo usados en apps móviles, páginas web, modelos predictivos, visualizaciones, tesis o periodismo de datos.	% de proyectos que aprovechan datos para el desarrollo de servicios, políticas, normas, planes, programas, proyectos o participar en asuntos de interés público.

4.Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto	
% de ejercicios de participación o colaboración que cuentan con sello de excelencia	Involucramiento de ciudadanos, usuarios y grupos de interés en el desarrollo de servicios, políticas, y normas

5.Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de tecnologías de la información y las comunicaciones
Proyectos e iniciativas de ciudades y territorios inteligentes que cuentan con sello de excelencia

Indicadores de Cumplimiento: buscan medir el cumplimiento de los habilitadores de la política: Arquitectura, Seguridad de la Información y Servicios Ciudadanos Digitales.

5.5. Anexo 5 – Indicadores de Cumplimiento: Arquitectura

ASPECTO	FORMULA DEL ASPECTO A MEDIR	VARIABLE 2018	FÓRMULA	ID PREGUNTA	PREGUNTA ASOCIADA A LA VARIABLE A MEDIR	OPCIONES DE RESPUESTA	FORMULA
Estrategia de TI	ID01=(Planeación Estratégica de TI + Seguimiento + Cumplimiento de la implementación de la Estrategia de TI+ Arquitectura Empresarial +Documentación de la Arquitectura Empresarial +Servicios de TI)/6	Planeación Estrategia de TI	(PR01+PR02)/2	PR01	¿Cuál es el estado del Plan Estratégico de TI (PETI)?	A. No lo tiene o está en proceso de construcción B. Lo formuló, pero no está actualizado C. Lo formuló y está actualizado	SI A = 0 SI B = 70 SI C = 100
				PR02	El Plan Estratégico de TI (PETI) incluye:	A. El portafolio o mapa de ruta de los proyectos B. La proyección del presupuesto, C. El entendimiento estratégico, D. El análisis de la situación actual, E. El plan de comunicaciones del PETI F. Todos los dominios del Marco de Referencia. G. Diagnostico Interoperabilidad H. Diagnostico Autenticación Electrónica I. Diagnostico Carpeta ciudadana. J Ninguna de las anteriores	SI A = +100/6 SI B = +100/6 SI C = +100/6 SI D = +100/6 SI E = +100/6 SI F= +100/6

5.6. Anexo 6 – Indicadores de Cumplimiento: Seguridad

ASPECTO A MEDIR	FÓRMULA DEL ASPECTO A MEDIR	TEMA	FÓRMULA DEL TEMA A MEDIR	ID PREGUNTA	PREGUNTA ASOCIADA AL TEMA A MEDIR	OPCIONES DE RESPUESTA	FORMULA
Evaluación y planificación de la seguridad de la información	(Diagnostico Seguridad y Privacidad de la Información+ Política del MSPI+ Roles y responsabilidades del MSPI+ Procedimientos del MSPI+ Gestión de activos de seguridad de la información+ Gestión de riesgos de seguridad y	Diagnostico Seguridad y Privacidad de la Información	PR01	PR01	¿La entidad realiza un diagnóstico de seguridad de la información?	a En Construcción b Cuenta con el diagnostico. c No se Tiene	SI A =50 SI B =100 SI C=0
		Política del MSPI	PR02	PR02	¿La entidad adopta una política de seguridad de la información?	a En Construcción b Adoptada. c No se Tiene	SI A =50 SI B =100 SI C=0
		Roles y responsabilidades del MSPI Procedimientos del MSPI	PR03	PR03	¿La entidad define roles y responsabilidades de seguridad de la información en entidad?	a En Construcción b Están definidos. c No se Tiene	SI A =50 SI B =100 SI C=0
		Procedimientos del MSPI	PR04	PR04	¿La entidad define y apropia procedimientos de seguridad de la información?	a En Construcción b Están definidos. c No se Tiene	SI A =50 SI B =100 SI C=0
		Gestión de activos de seguridad de	PR05	PR05	¿La entidad realiza gestión de activos de seguridad de la	a En Construcción b los gestiona. c No los gestiona	SI A =50 SI B =100 SI C=0

Mediciones de Calidad: a través del Sello de la Excelencia en Gobierno digital, se realizarán las mediciones de calidad de los productos y servicios digitales de las entidades públicas del Estado Colombiano.

El Sello de Excelencia fue creado a través del Decreto 2573 de 2014 y adoptado en la Resolución 2405 de 2016 (modificada posteriormente mediante Resolución 1443 de 2018), en donde se define como un modelo de certificación que busca garantizar la alta calidad de los servicios digitales del Estado Colombiano.

El Sello de Excelencia está organizado en 4 categorías:

1. Categoría servicios en línea: Certifica la calidad de los trámites y servicios en línea.
2. Categoría gobierno abierto: Certifican los conjuntos de datos abiertos y los ejercicios de participación por medios digitales.
3. Categoría capacidades de Gestión de TI: Certifica las capacidades institucionales y operativas de las entidades públicas..
4. Categoría Ciudades y territorios inteligentes: certifica la calidad de las iniciativas implementadas de ciudades o territorios inteligentes, que solucionan al menos una problemática de carácter urbano, social, ambiental, económico y político (ODS)

http://www.sellodeexcelencia.gov.co/

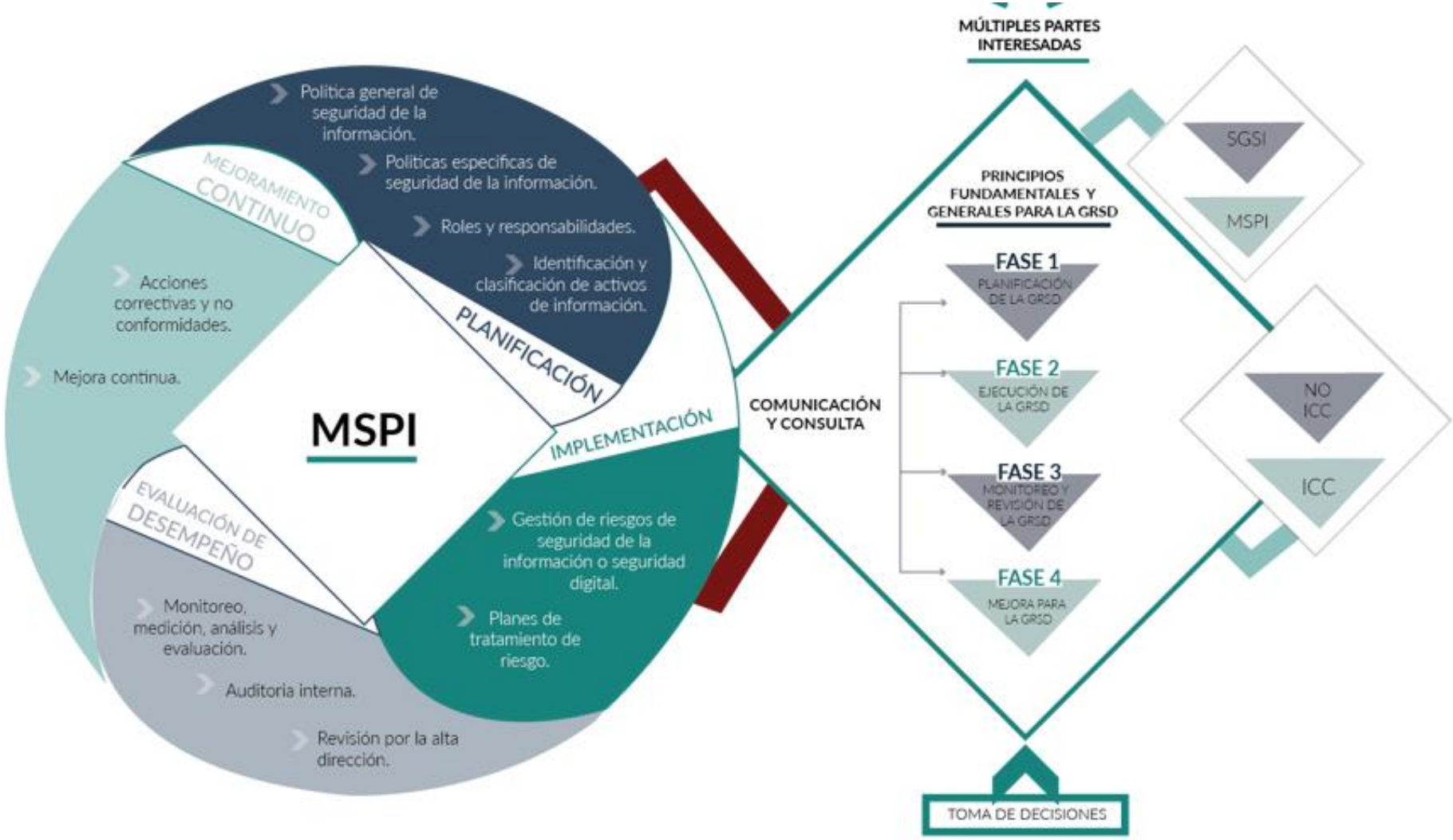
POLITICA DE SEGURIDAD DIGITAL

El propósito de esta política es contrarrestar el incremento de las amenazas informáticas que afecten significativamente, y afrontar retos en aspectos de seguridad cibernética.

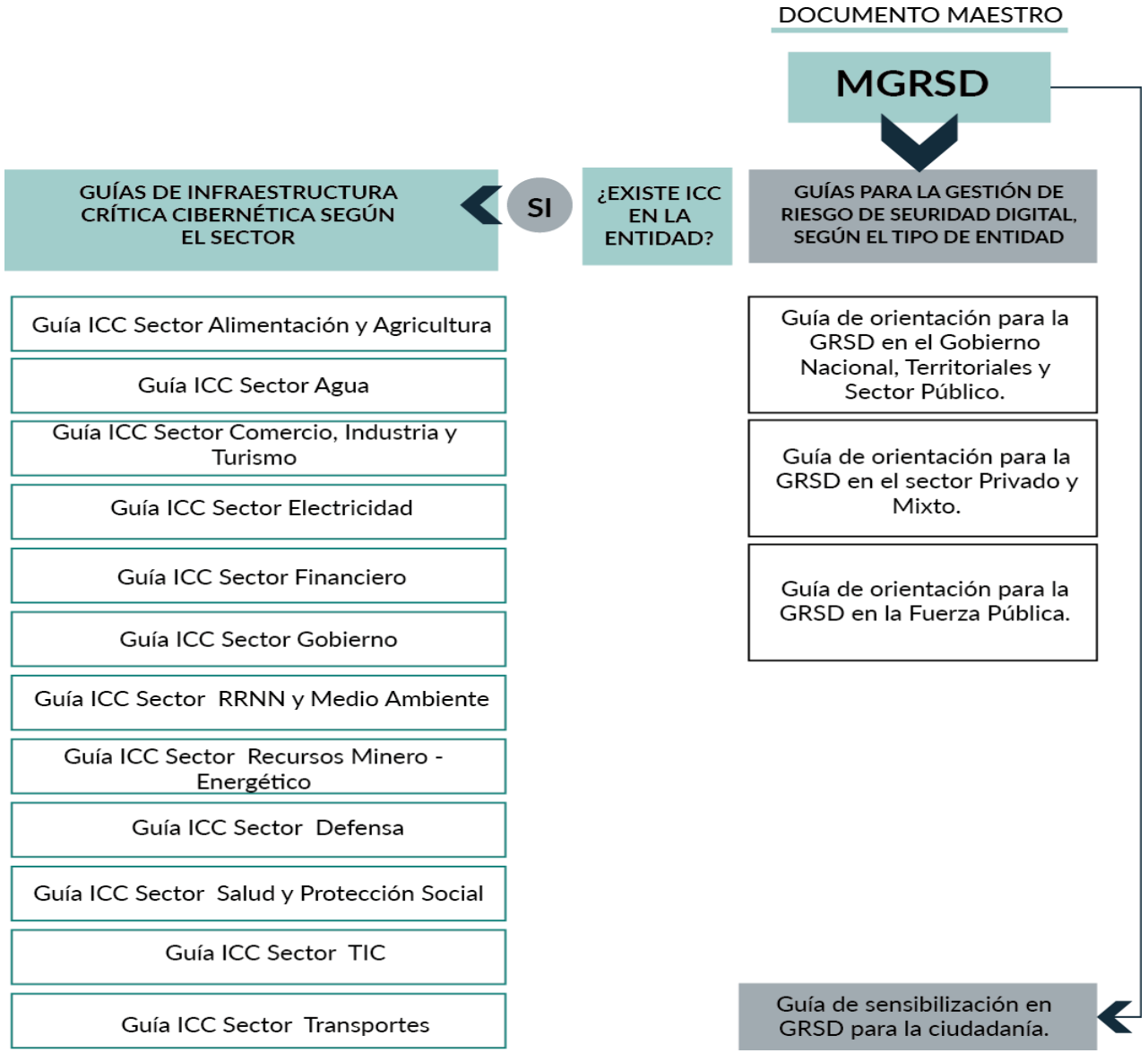
En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

En el orden territorial, MinTIC definirá los lineamientos para que las entidades territoriales definan la figura del enlace de Seguridad Digital territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) CON EL MODELO NACIONAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD)



El Modelo Nacional de Gestión de Riesgos de Seguridad Digital MNGRSD está estructurado como lo indica el siguiente gráfico:



MODELO NACIONAL DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD)

Planificación de la GRSD	Ejecución de la GRSD	Monitoreo y Revisión de la GRSD	Mejora de la GRSD
Consiste en la definición de contextos, variables para posterior análisis y evaluación de riesgos y en general todos los aspectos que se desarrollarán en los demás componentes	Consiste en el desarrollo de las actividades para el análisis y evaluación de los riesgos de seguridad digital, se identifican aspectos inherentes y residuales de los mismos, así como la definición del tratamiento de los riesgos en el marco de la seguridad de la información y particularmente en las ICC.	Consiste en la permanente evaluación que permita asegurar que dicha gestión se está llevando a cabo bajo los aspectos y lineamientos definidos por cualquier entidad para sus riesgos de seguridad digital. Se desprenden aspectos de reporte y aseguramiento del seguimiento de todos los planes de tratamiento que se derivan de su aplicación.	Componente que tiene una orientación para establecer los mecanismos que permitan alcanzar un mayor grado de madurez de la GRSD en cualquier entidad.

FASE 1: PLANIFICACION

La fase de **planificación** comprende todo lo expuesto en los **Pasos 1, 2 y 3** de la *Guía para la Administración de los Riesgo de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública*, es decir, comprende todo lo relacionado con las siguientes actividades:

- Definición del contexto interno, externo y de los procesos de la entidad pública.
- Definición de la política de administración de riesgo.
- Designación de roles y responsabilidades
- Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable.
- Identificación de activos de Seguridad Digital
- Identificación de riesgos.
- Valoración de riesgos.
- Definición del tratamiento de los riesgos.

RESPONSABLE DE SEGURIDAD DIGITAL

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Identificación de activos de Seguridad Digital

Son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

Es necesario que la entidad pública **identifique los activos y documente un inventario de activos**, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

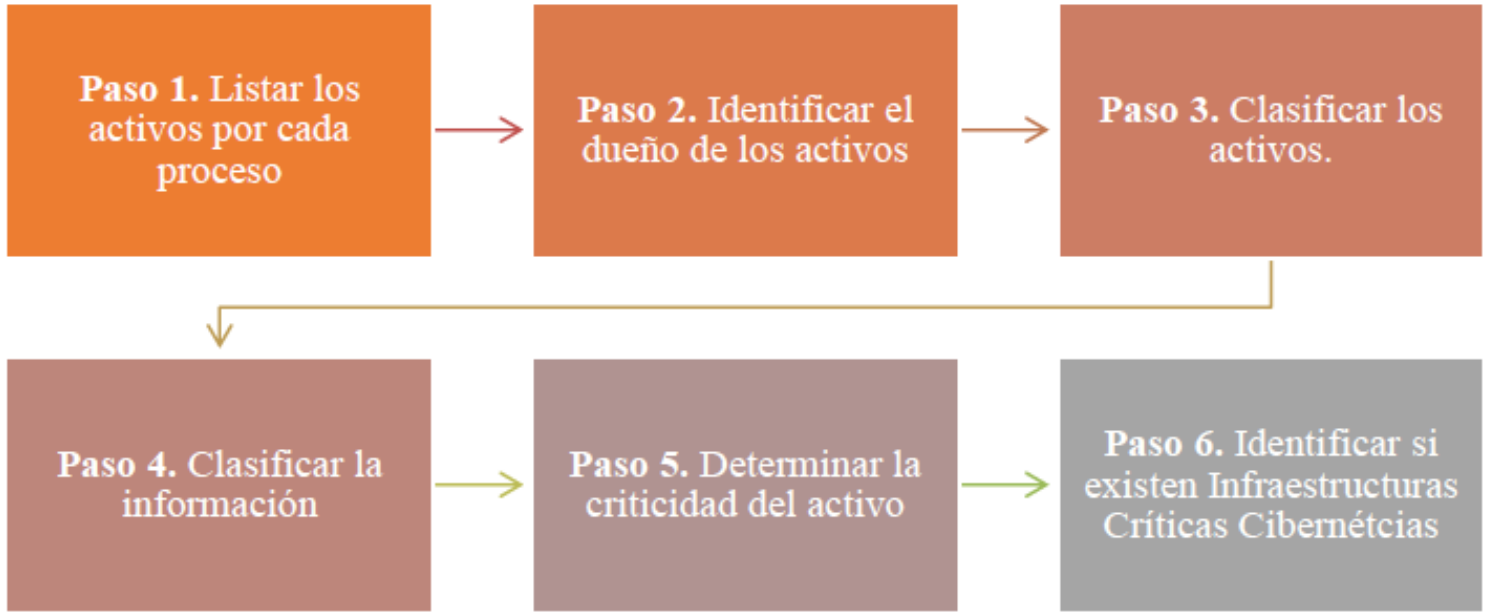


Imagen 2. Pasos para la identificación y valoración de activos.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Identificar los riesgos inherentes de seguridad digital

Como lo indica el **Paso 2** de la "*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas*" emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles **amenazas** y **vulnerabilidades** que podrían causar su materialización.

Tabla 5. Tabla de amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: ISO/IEC 27005:2009

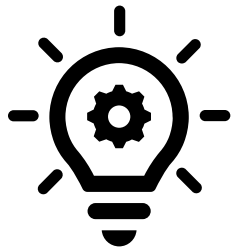
Tabla 7. Tabla de Vulnerabilidades Comunes

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso

Tabla 8. Tabla de Amenazas y Vulnerabilidades

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones



FASE 2: EJECUCION

1

- Se centra en la implementación de los planes de tratamiento de riesgos definidos en la fase anterior, en esencia es seguir la ruta crítica definida y llevar a cabo todo lo planeado en la Fase 1.

2

- Aquí la Línea Estratégica debe cumplir con el compromiso de brindar los recursos necesarios para iniciar el tratamiento de los riesgos.

3

- El responsable de seguridad digital deberá supervisar y acompañar el proceso de implementación de los planes de tratamiento, verificando que los responsables de los planes (Primer Línea de Defensa y la Oficina de Tecnologías de la Información -TI- generalmente) ejecuten las tareas en los tiempos pactados y que los recursos se estén ejecutando de acuerdo con lo planeado

FASE 3. MONITOREO Y REVISIÓN

La entidad pública a través de las **Tres Líneas de defensa**, debe hacer un seguimiento a los planes de tratamiento para determinar su efectividad, de acuerdo con lo definido a continuación:

Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción.	Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario.	Realizar monitoreo de los riesgos y controles tecnológicos
Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.	Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.	Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

Todo lo anterior contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la línea estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y las partes interesadas.

Registro y reporte de incidentes de seguridad digital

Es importante que la entidad pública cuente con el registro de los incidentes de seguridad digital que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.

El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

Reporte de la gestión del riesgo de seguridad digital al interior de la entidad pública

El responsable de seguridad digital debería reportar periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la siguiente información:

REPORTE

1. Matriz de los riesgos identificados de seguridad digital.
2. Listado de activos críticos TI/TO y listado de ICC.
3. Reporte de criticidad/Impacto de la organización.
4. Plan de tratamiento de riesgos.
5. Reporte de evolución de riesgos y modificación del apetito de riesgo.
6. Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de evaluación realizada.
7. Impacto económico que podría presentarse frente a la materialización de los riesgos.

PERIODICIDAD

- Periódicamente por parte de todas las Entidadaes u organizaciones que han adaptado el modelo respectivo.
- Cuando ocurra un cambio organizacional o de los procesos de la organización que genere de un impacto en la operaciones o que pueda afectar los riesgos ya identificados anteriormente. En este caso debe realizarse una nueva evaluación de los riesgos y reportar los resultados a la Entidad de control
- Cuando se incluya un nuevo proceso dentro del alcance de la gestión de riesgos de seguridad digital de la organización.En este acaso se debe realizar una nueva evaluación de riesgosy reportar los resultados a la Entidad de control.

Reporte de la gestión del riesgo de seguridad digital a autoridades o entidades especiales

La finalidad del reporte de esta información es que el Gobierno Nacional pueda identificar posibles oportunidades para la generación de política pública, generación de capacidades o asignación de recursos que permita ayudar a la mejora de la seguridad digital.

Se propone que las entidades públicas consoliden la siguiente información puntual para poder llevar a cabo el reporte respectivo:

- Riesgos con nivel crítico
- Amenazas críticas
- Vulnerabilidades críticas
- Tipos de Activos afectados por los riesgos críticos
- Planes de tratamiento propuestos para la mitigación y si han sido ejecutados
- Servicios digitales críticos en la entidad pública

Auditorías internas y externas

Le corresponde a las **Unidades de Control Interno (tercera línea de defensa)**, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo de seguridad digital en la entidad pública, catalogándola como una unidad auditable más dentro de su Universo de Auditoría, conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

Medición del desempeño

La entidad pública debe utilizar medidas de desempeño (indicadores) para la gestión de los riesgos de seguridad digital, las cuales deben reflejar el cumplimiento de los objetivos propuestos.

Estas deben ser evaluadas periódicamente alineadas con la revisión por la línea estratégica.

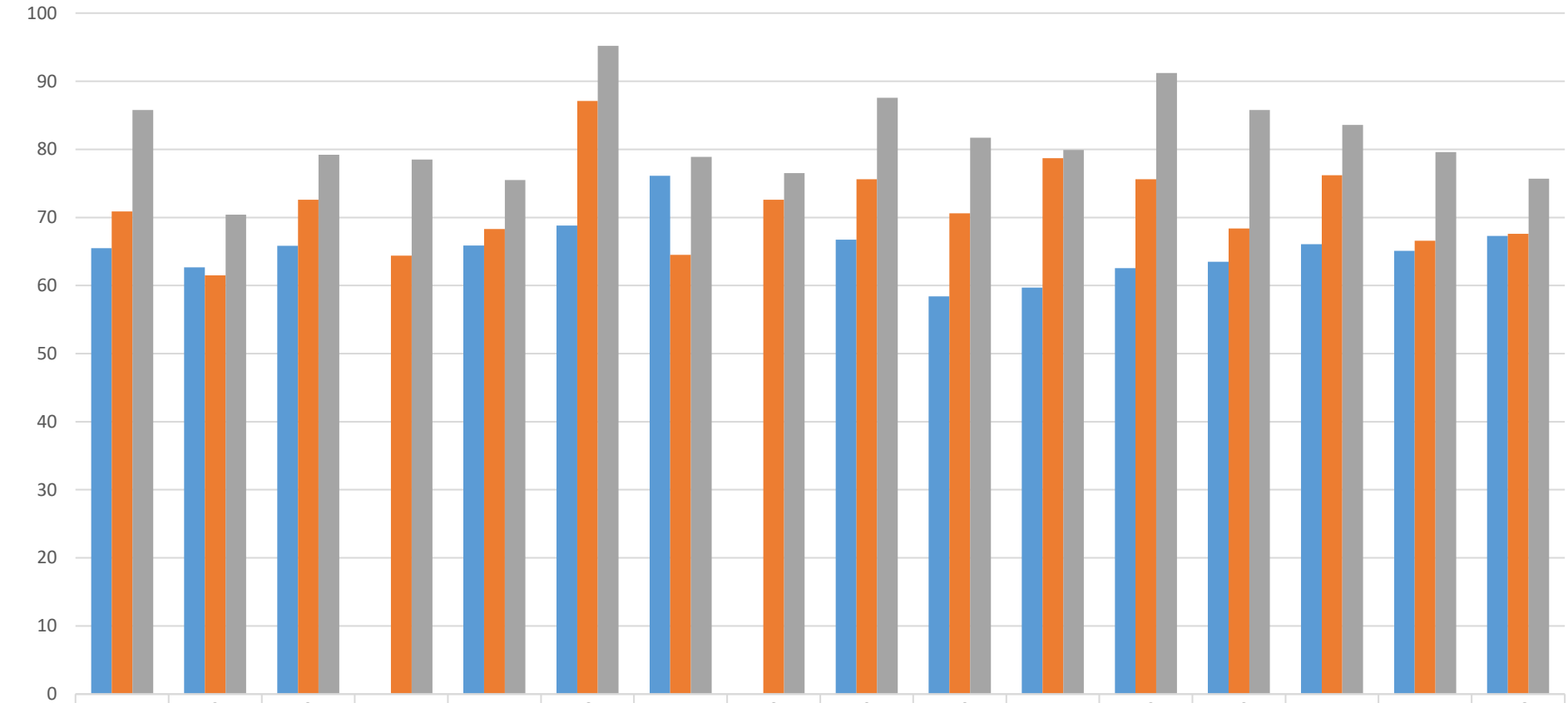
FASE 4. MEJORAMIENTO CONTINUO DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Deben definirse las acciones para mejorar continuamente la gestión de riesgos de seguridad digital de la siguiente forma:

- Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas.
- Establecer las posibles causas y consecuencias del hallazgo.
- Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar.
- Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

2. RESULTADOS DEL FURAG

Resultados de la Gestión y Desempeño -Administración Departamental del Quindío por Política vigencias 2017, 2018 Y 2019



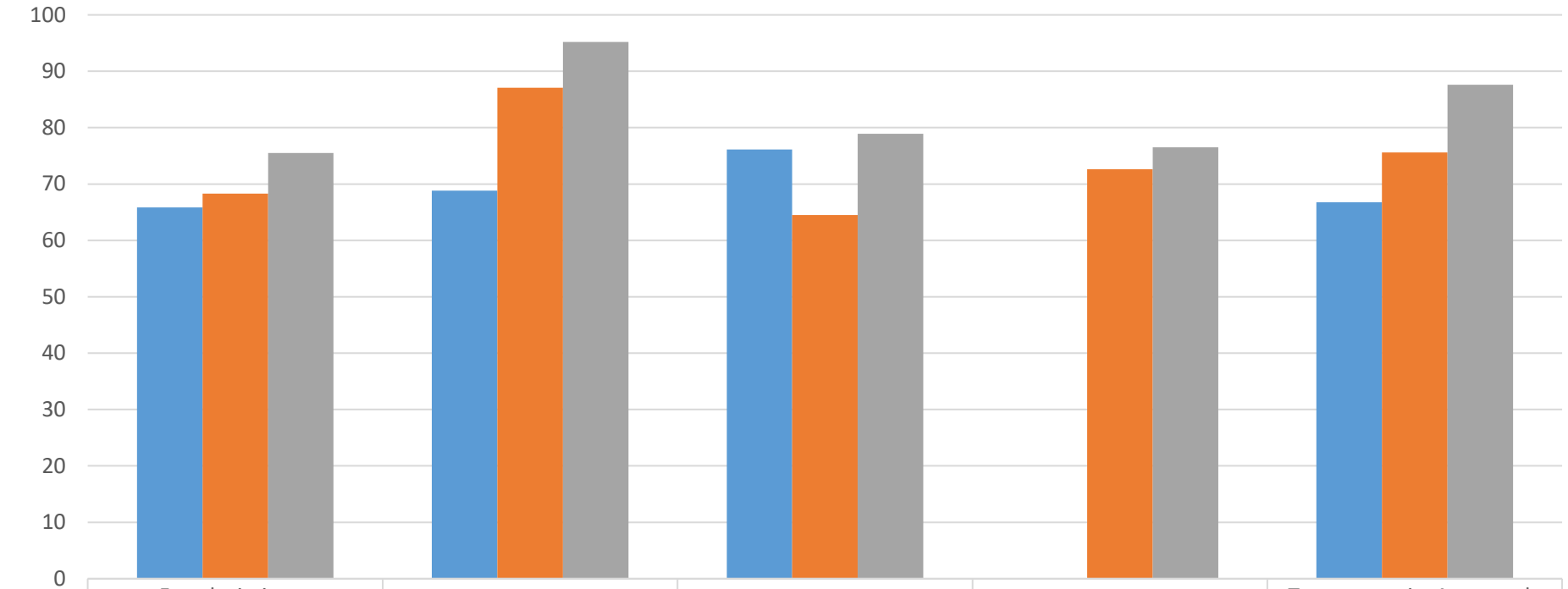
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2017	65,48	62,68	65,83		65,86	68,83	76,11		66,75	58,4	59,7	62,56	63,49	66,07	65,08	67,28
2018	70,9	61,5	72,6	64,4	68,3	87,1	64,5	72,6	75,6	70,6	78,7	75,6	68,4	76,2	66,6	67,6
2019	85,8	70,4	79,2	78,5	75,5	95,2	78,9	76,5	87,6	81,7	79,9	91,2	85,8	83,6	79,6	75,7

Fuente: Departamento Administrativo de la Función Pública DAFP- FURAG 2017, 2018 Y 2019

POL01: Gestión Estratégica del Talento Humano	POL05: Fortalecimiento Organizacional y Simplificación de Procesos	POL09: Transparencia, Acceso a la Informa lucha contra la Corrupción	POL13: Seguimiento y Evaluación del Desempeño Institucional
POL02: Integridad	POL06: Gobierno Digital	POL10: Servicio al ciudadano	POL14: Gestión Documental
POL03: Planeación Institucional	POL07: Seguridad Digital	POL11: Racionalización de Trámites	POL15: Gestión del Conocimiento
POL04: Gestión Presupuestal y Eficiencia del Gasto Público	POL08: Defensa Jurídica	POL12: Participación Ciudadana en la Ges Pública	POL16: Control Interno

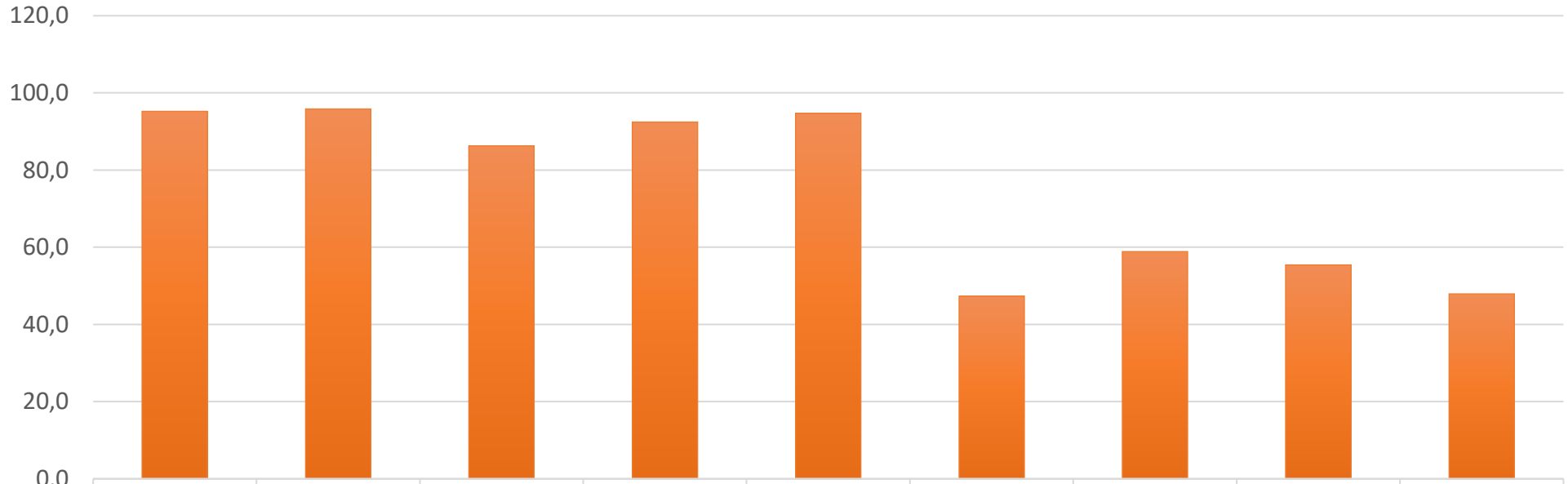
Departamento del Quindío

DIMENSION GESTIÓN PARA RESULTADOS CON VALORES (2)



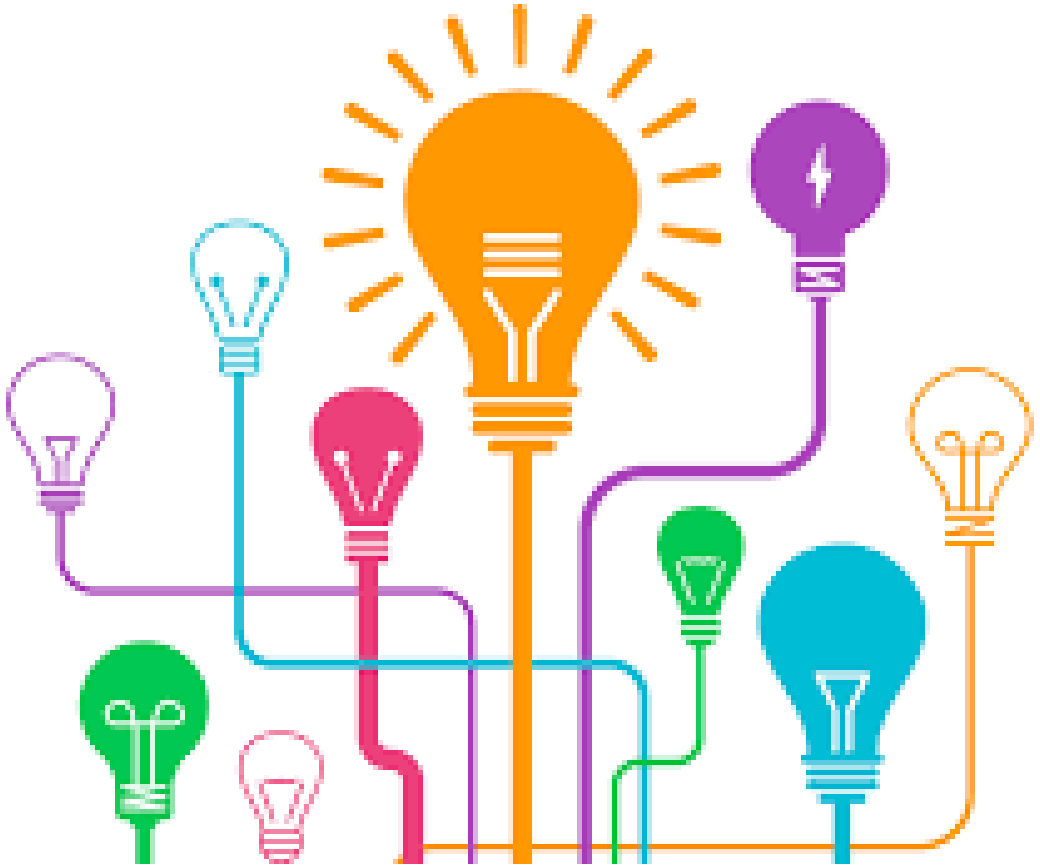
	Fortalecimiento organizacional y simplificacion de procesos	Gobierno Digital	Seguridad Digital	Defensa Juridica	Transparencia, Acceso a la Informacion Publica y Lucha contra la corrupcion
2017	65,86	68,83	76,11		66,75
2018	68,3	87,1	64,5	72,6	75,6
2019	75,5	95,2	78,9	76,5	87,6

COMPONENTES POLÍTICA GOBIERNO DIGITAL



	POLÍTICA 6 Gobierno Digital	I18GOBIERNO DIGITAL Empoderamiento de los ciudadanos mediante un Estado abierto	I19GOBIERNO DIGITAL Servicios Digitales de Confianza y Calidad	I20GOBIERNO DIGITAL Fortalecimiento de la Arquitectura Empresarial y de la Gestión de TI	I21GOBIERNO DIGITAL Fortalecimiento de la Seguridad y Privacidad de la Información	I82 GOBIERNO DIGITAL Procesos seguros y eficientes	I83 GOBIERNO DIGITAL Toma de decisiones basadas en datos	I84 GOBIERNO DIGITAL Impulso en el desarrollo de territorios y ciudades inteligentes	I85 GOBIERNO DIGITAL Uso y apropiación de los Servicios Ciudadanos Digitales
2019	95,2	95,8	86,3	92,5	94,7	47,3	58,9	55,5	47,9

3. RECOMENDACIONES Y PLAN DE ACCION



Recomendaciones de mejora para Gobierno Digital

1	Incluir la definición de la situación objetivo y modelo de gestión de TI en el Plan Estratégico de Tecnologías de la Información (PETI).
2	Definir herramientas tecnológicas para la gestión de proyectos de TI de la entidad.
3	Incluir características en los sistemas de información de la entidad que permitan la apertura de sus datos de forma automática y segura.
4	Elaborar y actualizar los documentos de arquitectura de los desarrollos de software de la entidad.
5	Definir e implementar una metodología de referencia para el desarrollo de software y sistemas de información.
6	Definir un proceso de construcción de software que incluya planeación, diseño, desarrollo, pruebas, puesta en producción y mantenimiento.
7	Implementar un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información que incluya criterios funcionales y no funcionales.
8	Definir y aplicar una guía de estilo en el desarrollo de los sistemas de información de la entidad e incorporar los lineamientos de usabilidad definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.
9	Adoptar en su totalidad el protocolo IPV6 en la entidad.
10	Elaborar un documento de diseño detallado de la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.

Recomendaciones de mejora para Gobierno Digital

11	Elaborar informes de las pruebas piloto realizadas para la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
12	Elaborar informes de activación de políticas de seguridad para la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
13	Elaborar un documento de pruebas de funcionalidad para la implementación del Protocolo de Internet versión 6 (IPV6) en la entidad.
14	Elaborar un acta de cumplimiento a satisfacción de la entidad sobre el funcionamiento de los elementos intervenidos en la fase de implementación del Protocolo de Internet versión 6 (IPV6).
15	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
16	Habilitar funcionalidades que permitan a los usuarios hacer seguimiento al estado de los trámites disponibles en línea o parcialmente en línea.
17	Habilitar funcionalidades que permitan a los usuarios hacer seguimiento al estado de los otros procedimientos administrativos disponibles en línea o parcialmente en línea.
18	Mejorar los trámites en línea de la entidad teniendo en cuenta las necesidades de los usuarios, con el propósito de aumentar su nivel de satisfacción.
19	Ejecutar al 100% los proyectos de TI que se definen en cada vigencia.
20	Disponer en línea todos los trámites de la entidad, que sean susceptibles de disponerse en línea.

Recomendaciones de mejora para Gobierno Digital

21	Disponer en línea los otros procedimientos administrativos de la entidad, que sea susceptibles de disponerse en línea.
22	Caracterizar los usuarios de todos los otros procedimientos administrativos de la entidad que están disponibles en línea y parcialmente en línea.
23	Cumplir con todos los criterios de accesibilidad web, de nivel A y AA definidos en la NTC5854, para todos los otros procedimientos de la entidad disponibles en línea y parcialmente en línea.
24	Cumplir los criterios de usabilidad web para todos los otros procedimientos administrativos de la entidad que están disponibles en línea y parcialmente en línea.
25	Promocionar los otros procedimientos administrativos disponibles en línea y parcialmente en línea para incrementar su uso.
26	Emplear diferentes medios digitales en los ejercicios de participación realizados por la entidad.
27	Mejorar las actividades de elaboración de normatividad mediante la participación de los grupos de valor en la gestión de la entidad.
28	Mejorar las actividades de racionalización de trámites mediante la participación de los grupos de valor en la gestión de la entidad.
29	Mejorar la solución de problemas a partir de la implementación de ejercicios de innovación abierta con la participación de los grupos de valor de la entidad.

Recomendaciones de mejora para Seguridad Digital

1	Establecer una periodicidad para el seguimiento al manejo de riesgos dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
2	Establecer el nivel de aceptación del riesgo dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
3	Establecer niveles para calificar el impacto del riesgo dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
4	Incorporar el análisis del contexto interno y externo de la entidad dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.
5	Fomentar por parte del comité institucional de coordinación de control interno la divulgación e implementación de la política de administración del riesgo.
6	Monitorear por parte del comité institucional de coordinación de control interno el seguimiento a la gestión del riesgo por parte de las instancias responsables para determinar si este se lleva a cabo adecuadamente.
7	Fomentar por parte del comité institucional de coordinación de control interno la promoción de los espacios para capacitar a los líderes de los procesos y sus equipos de trabajo sobre la metodología de gestión del riesgo con el fin de que sea implementada adecuadamente entre los líderes de proceso y sus equipos de trabajo.
8	Fomentar por parte del comité institucional de coordinación de control interno la generación de acciones para apoyar la segunda línea de defensa frente al seguimiento del riesgo.
9	Establecer controles para evitar la materialización de riesgos de seguridad y privacidad de la información.
10	Actualizar sus mapas de riesgos de acuerdo a los resultados del monitoreo o seguimiento.

Recomendaciones de mejora para Seguridad Digital

11	Divulgar oportunamente la actualización de sus mapas de riesgos.
12	Asegurar por parte de los cargos que lideran de manera transversal temas estratégicos de gestión (tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, líderes de otros sistemas de gestión, comités de riesgos) que los riesgos identificados son monitoreados de acuerdo con la política de administración de riesgos.
13	Hacer seguimiento por parte de Los cargos que lideran de manera transversal temas estratégicos de gestión (tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, líderes de otros sistemas de gestión, comités de riesgos) a los mapas de riesgos y verificar que se encuentren actualizados.
14	Proponer por parte de los cargos que lideran de manera transversal temas estratégicos de gestión (tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, líderes de otros sistemas de gestión, comités de riesgos)acciones de mejora para el diseño o ejecución de los controles.
15	Llevar a cabo una gestión del riesgo que le permita controlar los puntos críticos de éxito.
16	Llevar a cabo una gestión del riesgo que le permita ejecutar los controles de acuerdo con su diseño.
17	Llevar a cabo una gestión del riesgo que le permita garantizar de forma razonable el cumplimiento de los objetivos de los procesos.
18	Verificar por parte de la alta dirección o el comité institucional de control interno que se estén llevando a cabo evaluaciones de gestión, incluida la gestión del riesgo.
19	Analizar por parte de la alta dirección o el comité institucional de control interno el estado del sistema de control interno (SCI) y determinar los ajustes o modificaciones a que haya lugar.
20	Informar periódicamente por parte de los líderes de los programas, proyectos, o procesos de la entidad en coordinación con sus equipos de trabajo, a las instancias correspondientes sobre el desempeño de las actividades de gestión de riesgos.

Recomendaciones de mejora para Seguridad Digital

21	Identificar por parte de los líderes de los programas, proyectos, o procesos de la entidad en coordinación con sus equipos de trabajo, deficiencias en los controles y proponer los ajustes necesarios a los mismos.
22	Contemplar en la evaluación a la gestión del riesgo que hacen los jefes de planeación, líderes de otros sistemas de gestión o comités de riesgos, la elaboración de informes para la alta dirección sobre el monitoreo a los indicadores de gestión, determinando el alcance de los objetivos y metas institucionales.
23	Contemplar en la evaluación a la gestión del riesgo que hacen los jefes de planeación, líderes de otros sistemas de gestión o comités de riesgos, la elaboración de informes a las instancias correspondientes sobre las deficiencias de los controles.
24	Contemplar por parte del Jefe de Control Interno que sus informes de seguimientos y auditoria contribuyan en el diseño y ejecución de acciones de mejora enfocadas al cumplimiento de los objetivos y metas institucionales.
25	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.

Recomendaciones de mejora para Seguridad Digital

26	Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en los ejercicios de simulación nacional o internacional para desarrollar habilidades y destrezas en materia de seguridad digital.
27	Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital.
28	Reconocer como instancias de la política de seguridad digital al CSIRT de Gobierno y otros CCIRT.
29	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética.
30	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en las mesas de construcción y sensibilización del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.

5. PREGUNTAS

CONTACTO

GLORIA EUGENIA CASTAÑO

Contratista
Secretaría de Planeación Departamental

E-mail: mipgquindio@gmail.com
Cel.: ++ 304 653 4009

TÚ Y YO Somos Quindío

GOBERNACIÓN DEL QUINDÍO

¡GRACIAS!

Departamento del Quindío

QUINDÍO
CORAZÓN DEL PAISAJE CULTURAL CAFETERO

PAISAJE CULTURAL CAFETERO

TÚ Y YO Somos Quindío
Departamento del Quindío
QUINDÍO
PAISAJE CULTURAL CAFETERO