SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMAION SGSI – GOBERNACION DEL CESAR - 2022

Detalle del Documento	
Nombre de Documento	Plan de seguridad y privacidad de dad de la Información
Versión del Documento	1.2
Fecha	10/12/2021
Detalle	Este habilitador 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 con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información.

Control de Cambios		
Fecha	**Versión**	**Descripción**
10/12/2021	1.2	Seguimiento

Control de Aprobación			
Variables	**Fecha**	**Nombre**	**Cargo o Perfil**
Elaboró	10/12/2021	Alex Gómez Garzón	Ing. Sistemas
Revisó	10/12/2021	Alfonso García. P	Ing. Sistemas
Aprobó	30/12/2021	Comité de Gestión y Desempeño	

TABLA DE CONTENIDO

1. GENERALIDADES – CONOCIMIENTO DE LA ENTIDA

1.1 Introducción.

La política del gobierno nacional en el marco de Decreto 1078 del 2015 “Decreto único reglamentario del sector TIC” y en cumplimiento del decreto 1008 de 2018, que establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, con el objetivo de Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”.

El gobierno nacional a través del Plan Nacional de Desarrollo 2018 – 2022 “Pacto por Colombia pacto por la Equidad”, establece la importancia de las tecnologías de la información y comunicaciones como fuente y pilar para el desarrollo de las regiones de Colombia, para ello, el Plan TIC 2019 – 2022 “El futuro digital es de todos”, establece cuales son las directrices y lineamientos que las entidades públicas deben tener en cuenta para el desarrollo y fortalecimiento institucional de las TIC.

Para la implementación de la Política de Gobierno Digital, se han definido dos componentes: TIC para el Estado y TIC para la Sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

Seguridad de la Información: Este habilitador 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 con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información, así como la protección de los datos personales que tratan las entidades públicas en cumplimiento de la normatividad de protección de datos personales. Este habilitador tiene su soporte en el MSPI, que contempla 6 niveles de madurez.

Los habilitadores transversales de la política de Gobierno Digital: Arquitectura, Seguridad de la Información y Servicios Ciudadanos Digitales; son elementos fundamentales que permiten el despliegue de los componentes de la política y tienen como objetivo, desarrollar capacidades en cada entidad para la implementación de la política.

Por ello, de manera paralela a la implementación de los componentes (TIC para el Estado y TIC para la Sociedad), la entidad debe trabajar en el desarrollo de los elementos habilitadores que se definen de la siguiente forma:

El Departamento del Cesar, en cumplimiento a las Políticas y Directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Decreto
612 del 4 de Abril de 2018, Decreto 1078 implementará actividades de planeación estratégica para el control y administración efectiva de los riesgos y las necesidades de seguridad de la información de la entidad.

Una vez socializado el presente plan, los funcionarios, contratistas y terceros de la entidad adoptarán los controles de seguridad y privacidad de la información en sus procesos, con el fin de minimizar los riesgos que puedan afectar la seguridad y privacidad de la información

1.2 Objetivo general

Implementar estrategias que permitan garantizar la seguridad de la información de la Gobernación del Departamento del Cesar en cada uno de sus pilares (Integridad, Disponibilidad y Confidencialidad).

1.3 Objetivos específicos

- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de planificación.
- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de implementación.
- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de evaluación y desempeño.
- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de mejora continua

1.4 Alcance

Aplica a todos los Procesos de la entidad, a los líderes de cada proceso, al custodio y propietario de la información, y terceros que en razón del cumplimiento de sus funciones y las del Departamento compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Plan aplica a toda la información creada, procesada o utilizada por la entidad, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

1.5 Marco normativo

Marco Normativo		
N°	**Marco Normativo**	**Descripción**
1	**Decreto 1151 de 2008**	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
2	**Ley 1955 del 2019**	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones (Min TIC)
3	**Ley 1273 de 2009**	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
4	**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 del Espectro y se dictan otras disposiciones.
5	**Ley 1581 de 2012**	Por la cual se dictan disposiciones generales para la protección de datos personales.
6	**Ley 1712 de 2014**	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
7	**Ley 1753 de 2015**	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "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.
8	**Ley 962 de 2005**	El artículo 14 lo siguiente “Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario.
9	**Decreto 1413 de 2017**	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
10	**Decreto 2150 de 1995**	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
11	**Decreto 4485 de 2009**	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
12	**Decreto 235 de 2010**	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.

13	**Decreto 2364 de 2012**	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
14	**Decreto 2693 de 2012**	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.
15	**Decreto 1377 de 2013**	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos personales
16	**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
17	**Decreto 2433 de 2015**	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
18	**Decreto 1078 de 2015**	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
19	**Decreto 103 de 2015**	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
20	**Decreto 415 de 2016**	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 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.
21	**Decreto 1499 de 2017**	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
22	**Decreto 612 de 2018**	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
23	**Decreto 1008 de 2018**	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
24	**Decreto 2106 del 2109**	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva
25	**Decreto 620 de 2020**	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
26	**Resolución 2710 de 2017**	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
27	**Resolución 3564 de 2015**	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
28	**Resolución 3564 2015**	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
29	**Norma Técnica Colombiana NTC 5854 de 2012**	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
30	**CONPES 3292 de 2004**	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir deasociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos
31	**Conpes 3920 de Big Data, del 17 de abril de 2018**	La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles
32	**Conpes 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016**	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
33	**Conpes 3975**	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
34	**Circular 02 de 2019**	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
35	**Directiva 02 2019**	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

1.6 Base Metodológica

- Norma ISO/IEC 27001:2013.
- Modelo de Seguridad y Privacidad de la Información de Gobierno Digital –MSPI
- Instrumento de Evaluación MSPI MINTIC

1.7 Definiciones

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ALCANCE: ámbito de la organización que queda sometido al SGSI.

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

ANÁLISIS DE RIESGOS: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

ANÁLISIS DE RIESGOS CUALITATIVO: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

ANÁLISIS DE RIESGOS CUANTITATIVO: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

CONTROL CORRECTIVO: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

CONTROL DETECTIVO: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

CONTROL DISUASORIO: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.
CONTROL PREVENTIVO: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

ESTIMACIÓN DE RIESGOS: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

EVALUACIÓN DE RIESGOS: Proceso global de identificación, análisis y estimación de riesgos.

FASE DIAGNOSTICO: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

FASE EVALUACIÓN DE DESEMPEÑO (VERIFICAR**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

FASE IMPLEMENTACIÓN (HACER): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

FASE PLANIFICACIÓN (PLANEAR**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

FASE MEJORA CONTINUA (ACTUAR**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

GESTIÓN DE RIESGOS: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INVENTARIO DE ACTIVOS: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

ISO/IEC 27001:2013: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI): El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

RIESGO RESIDUAL: El riesgo que permanece tras el tratamiento del riesgo.

SELECCIÓN DE CONTROLES: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora contínua.

2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La gobernación del Departamento del Cesar para la documentación del plan de seguridad de la información se basó en el modelo PHVA que se encuentra en la guía “Plan de seguridad de la información” y el anexo N° 1 del Modelo de Seguridad y Privacidad de la información de MINTIC.

Este modelo consta de cuatro fases y una fase previa a la implementación

Modelo PHVA aplicado al MSPI	
PLANIFICAR (establecer el MSPI)	Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
HACER (implementar y operar el MSPI)	Implementar y operar la política, los controles, procesos y procedimientos del MSPI
VERIFICAR (hacer seguimiento y revisar el MSPI)	Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
ACTUAR (mantener y mejorar el MSPI)	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.
(*.* Fuente: Guía plan de seguridad de la información - Min tic)	

Antes de la fase de planificación se debe tener en cuenta la fase de diagnóstico, que es una fase previa a la planificación, para la fase de diagnóstico se debe tener en cuenta el Instrumento de Evaluación del Modelo de Seguridad y privacidad de la información

2.1 Fase I. diagnóstico – etapa previas a la implementación

SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI						
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN						
FASE I. DIAGNÓSTICO – ETAPAS PREVIAS A LA IMPLEMENTACIÓN						
N°	ACTIVIDADES	RESPONSABLES	REGISTROS	FECHA INICIO	FECHA FINAL	REALIZADO
1	Fortalecer el estado actual de la gestión de seguridad y privacidad de la información al interior de mla interior de la Entidad.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI – MINTIC	01/01/2018	28/02/2018	100%
2	Mantener y Fortalecer el nivel de madurez de seguridad y privacidad de la información en la Entidad	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI – MINTIC	01/03/2018	30/04/2018	100%
3	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI – MINTIC	01/05/2018	31/12/2018	100%
4	Identificar el avance de la implementación del ciclo de operación al interior de la entidad.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI – MINTIC	01/07/2018	30/07/2018	100%
5	Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI – MINTIC Política de protección de datos personales – Decreto 00222 del 22 de Agosto de 2019	01/08/2018	30/08/2018	100%
6	Identificar y fortalecer el uso de buenas prácticas en ciberseguridad.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI – MINTIC	01/08/2018	30/08/2018	100%

2.2 Fase II. Planificación

SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI	
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
FASE. II. PLANIFICACIÓN – ETAPAS PREVIAS A LA IMPLEMENTACIÓN	
	CRONOGRAMA

	ACTIVIDADES	RESPONSABLES	REGISTROS	FECHA INICIO	FECHA FINAL	REALIZA DO
1	Fortalecer la Política de seguridad y privacidad de la información	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos	Documento con la política de seguridad de la información, aprobado por la alta Dirección y socializada al interior de la Entidad.	01/02/2021	31/12/2021	100%
2	Fortalecer los Procedimientos de seguridad de la información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos	Procedimientos, debidamente documentados, socializados y aprobados por el Comité Institucional de Gestión y Desempeño.	01/02/2021	31/12/2021	100%
3	Roles y responsabilidades de seguridad y privacidad de la información.	Comité Institucional de Gestión y Desempeño	Acto administrativo a través del cual se crea o se modifica las funciones del comité institucional de gestión y desempeño (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	01/02/2021	31/12/2021	100%
4	Fortalecimiento en la identificación del Inventario de activos de información.	Secretaría General - Comité Institucional de Gestión y Desempeño	Matriz con la identificación, valoración y clasificación de activos de información.	04/02/2020	31/12/2020	100%
5	Fortalecer la Integración del MSPI con el Sistema de Gestión documental	Secretaría General	Documentación de Plan de Preservación Digital	04/02/2020	31/12/2020	100%
6	Fortalecer la identificación, Valoración y tratamiento de riesgo de seguridad de información	Comité Institucional de Gestión y Desempeño	Documento con la metodología de gestión de riesgos de seguridad de información, con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos de seguridad de información, debidamente aprobado por Comité Institucional de Gestión y Desempeño	04/02/2020	31/12/2020	100%
7	Plan de Comunicaciones	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con el plan de comunicación sensibilización y capacitación para la entidad.	04/02/2020	31/12/2020	100%
8	Plan de transición Pv4 a IPv6. Fase I. PLANEACION	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documentación Fase I. PLANEACIÓN IPv4 a IPv6.	01/02/2020	31/12/2020	100%
	Plan de transición Pv4 a IPv6. Fase. III PRUEBAS DE FUNCIONAMIENTO	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documentación IPv4 a IPv6. Fase. III PRUEBAS DE FUNCIONAMIENTO	02/02/2022	31/12/2022	0%

2.3 Fase III. Implementación

SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI	
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
FASE. III. IMPLEMENTACIÓN	
N°	CRONOGRAMA

	ACTIVIDADES	RESPONSABLES	REGISTROS	FECHA INICIO	FECHA FINAL	REALIZA DO
1	Formular el plan de tratamiento de riesgo de seguridad de información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documentar el plan de tratamiento de riesgo de seguridad de informacion	02/01/2022	31/12/2022	100%
2	Implementar el plan de tratamiento de riesgo de seguridad de información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Ejecucuón de la Fase I. Planificación de la gestión de riesgo de la seguridad de información.	02/01/2022	31/12/2022	0%
3	Imlementación de controles de seguridad de información	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con el plan de tratamiento de riesgos donde se detallen los controles y sus objetivos.	02/01/2022	31/12/2022	100%
4	Elaborar o Diseñar herramienta que permita medir la eficacia de los controles de seguridad de la información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Formato.Doc o Formato.xls	02/01/2022	31/12/2022	0%
5	Implementar programas de formación o capacitación en materia de seguridad de información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registro de los funcionarios y contratistas capacitados	02/01/2022	31/12/2022	100%
6	Gestionar los recursos del MSPI	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Recurso Humano Recurso Tecnológico. Recurso Audiovisual. Recurso Impreso (Folletos, Afiches o pendones)	02/01/2022	31/12/2022	50%
7	Consolidar los reportes de incidentes de seguridad de información que se encuentren con un nivel de criticidad "ALTO" O "SUPERIOR"	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Reporte de incidentes de seguridad de información	02/01/2022	31/12/2022	0%
8	Indicadores De Gestión.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con la descripción de los indicadores de gestión de Seguridad y privacidad de la información.	02/01/2022	31/12/2022	0%
9	Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad de información	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Procedimientos, Controles o Políticas	02/01/2022	31/12/2022	100%
10	Plan de transición Pv4 a IPv6. Fase. II IMPLEMENTACION	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	IPv4 a IPv6. Fase II. IMPLEMENTACIÓN Documento aprobado con las estrategias del plan de implementación de IPv6	02/01/2022	31/12/2022	0%

2.4 Fase IV. Evaluación del desempeño

SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI						
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN						
FASE. IV. EVALUACIÓN Y DESEMPEÑO						
N°	CRONOGRAMA					
	ACTIVIDADES	RESPONSABLES	REGISTROS	FECHA INICIO	FECHA FINAL	REALIZADO
1	Seguimiento y revisión a la implementación del MSPI.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Seguimiento y revisión	02/01/2022	30/06/2022	100%
2	Seguimiento y revisión a la implementación del MSPI.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Seguimiento y revisión	01/07/2022	31/07/2022	100%
3	Realizar auditorías internas del MSPI a intervalos planificados	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Seguimiento y revisión	02/01/2022	31/12/2022	0%
4	Seguimiento y revisión a la Auditoria Interna de seguridad de información	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Seguimiento y revisión	02/01/2022	31/12/2022	0%
5	Seguimiento y revisión al cumplimiento de la política de seguridad de la información y Controles.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Seguimiento y revisión	02/01/2022	31/12/2022	0%

2.5 Fase V. Mejora continua

SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI						
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN						
FASE. V. MEJORA CONTINUA						
N°	CRONOGRAMA					
	ACTIVIDADES	RESPONSABLES	REGISTROS	FECHA INICIO	FECHA FINAL	REALIZADO
1	Mejorar uso de la política de seguridad de la información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Mejora y Actualización	02/01/2022	31/12/2022	80%
2	Mejorar los objetivos de seguridad de la información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Mejora y Actualización	02/01/2022	31/12/2022	90%
3	Mejora los resultados de la auditoría interna de seguridad de información	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Mejora y Actualización	02/01/2022	31/12/2022	0%
4	Mejorar el Uso e Implementación de los controles de seguridad de información	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Mejora y Actualización	02/01/2022	31/12/2022	90%
5	Mejorar el resultados de los indicadores	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Registros de Mejora y Actualización	02/01/2022	31/12/2022	80%