PLAN DE SEGURIDAD Y GOBIERNO DIGITAL
2025-2027

INTRODUCCIÓN

En el contexto actual, donde la información es uno de los activos más valiosos para las organizaciones, la protección de los datos y la privacidad se han convertido en pilares fundamentales para garantizar la confianza y el cumplimiento de las normativas vigentes.

En cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG) versión 6 y considerando las disposiciones de la Política de Gobierno Digital. Decreto 1008 de 2018 y la Política de Seguridad Digital CONPES 3995 de 2020; se realiza revisión técnica del documento "Plan de Seguridad Digital y Privacidad de la Información 2025".

El **Plan de Seguridad, Gobierno Digital y Privacidad de la Información 2025-2027** de la Empresa para la Seguridad y Soluciones Urbanas – ESU tiene como objetivo establecer un marco claro y eficaz para proteger la confidencialidad, integridad y disponibilidad de la información, así como asegurar que los datos personales y sensibles gestionados por la entidad sean tratados con el más alto nivel de seguridad.

Este plan esta alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional.

La Política de Gobierno Digital ha definido dos (2) componentes: TIC para el Estado y TIC para la Sociedad, y tres (3) habilitadores transversales: Arquitectura, Seguridad de la información y Servicios Ciudadanos Digitales.

Donde los componentes permiten mejorar el funcionamiento de las entidades públicas, su relación con otras entidades y el fortalecimiento de su relación con la sociedad. Los habilitadores por su parte, contribuyen al logro de los objetivos definidos en los componentes.

El habilitador de Seguridad y Privacidad, permite a la Empresa para la Seguridad y Soluciones Urbanas – ESU garantizar la confidencialidad, disponibilidad e integridad de la información, para lo cual se hace indispensable diseñar el Plan de Seguridad, Gobierno Digital y Privacidad de la Información que a continuación se detalla.

OBJETIVO GENERAL

Establecer directrices, políticas y procedimientos para proteger la información sensible y los datos personales gestionados por la entidad, garantizando su confidencialidad, integridad y disponibilidad. Este plan tiene como objetivo asegurar el cumplimiento de las normativas nacionales e internacionales en materia de protección de datos, mitigar los riesgos asociados a amenazas cibernéticas, salvaguardar la infraestructura tecnológica de la organización y promover la mejora continua de los servicios digitales, fortaleciendo la confianza, la eficiencia, la transparencia y el cumplimiento normativo.

OBJETIVOS ESPECÍFICOS

1. Fortalecer la gobernanza y seguridad de la información mediante políticas, controles y procedimientos que garanticen su confidencialidad, integridad, la disponibilidad, la gestión del riesgo y la continuidad del negocio.
2. Cumplir con las normativas en materia de protección de datos personales y ciberseguridad.
3. Promover el desarrollo de servicios ciudadanos digitales accesibles, seguros y centrados en el usuario.
4. Evaluar y mitigar los riesgos digitales, incluyendo la protección de infraestructuras críticas y respuesta a incidentes.

ALCANCE

El alcance de este plan es fortalecer la seguridad y gobierno digital en todos los procesos de la Empresa para la Seguridad y Soluciones Urbanas – ESU, abarcando todos los niveles funcionales y organizacionales. El enfoque está orientado a garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando que los servicios y sistemas que maneja la ESU se encuentren protegidos frente a amenazas y vulnerabilidades emergentes.

Este plan establecerá un marco robusto que permita la implementación de controles de seguridad efectivos y el desarrollo de protocolos de privacidad que salvaguarden los activos de información en toda la institución. A través de la adopción de buenas prácticas y el cumplimiento de normativas internacionales, como la ISO/IEC 27001:2022, mediante la cual se definen los requisitos de un Sistema de Gestión de la Seguridad de la Información-SGSI, se impulsará una cultura de mejora continua en la gestión de riesgos digitales.

Al finalizar la ejecución de este plan, la Empresa para la Seguridad y Soluciones Urbanas – ESU contará con procesos y procedimientos más maduros en términos de seguridad y privacidad de la información. Estos avances permitirán una mejor gestión de riesgos, un aumento en la resiliencia operativa, y la consolidación de un entorno tecnológico confiable y seguro para el cumplimiento de los objetivos institucionales.

NORMATIVIDAD Y METODOLOGÍA

La actualización del plan estratégico se define teniendo en cuenta el siguiente marco normativo:

Marco Normativo			
ID	**Fuente**	**Año**	**Descripción**
N001	Ley 152	1994	Por la cual se establece la Ley Orgánica del Plan de Desarrollo.
N002	Ley 489	1998	Por la cual se regula el ejercicio de la función administrativa, determina la estructura y define los

Marco Normativo			
			principios y reglas básicas de la organización y funcionamiento de la Administración Pública.
N003	Decreto 115	1996	Por el cual se establecen normas sobre la elaboración, conformación y ejecución de los presupuestos de las Empresas Industriales y Comerciales del Estado y de las Sociedades de Economía Mixta sujetas al régimen de aquellas, dedicadas a actividades no financieras.
N004	Decreto Municipal178	2002	Por medio del cual se transforma el Fondo Metropolitano de Seguridad - METROSEGURIDAD- en la Empresa Industrial y Comercial del Estado, del orden Municipal
N005	Ley 1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
N006	Ley 1437	2011	Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
N007	Ley 1581	2012	Lineamientos MinTIC para Gestión de Seguridad de la Información. Protección de Datos Personales
N008	Ley 1712	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.
N009	Decreto 1082	2015	Por medio del cual se expide el Decreto Único Reglamentario del sector administrativo de planeación nacional.
N010	Decreto 1499	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. Modelo Integrado de Planeación y Gestión (MIPG).
N011	Decreto 612	2018	Por el cual se fijan directrices para la integración de planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
N012	Decreto 1008	2018	Política de Gobierno Digital.
N013	CONPES 3995	2020	Política Nacional de Confianza y Seguridad Digital.
N014	CONPES 4441	2025	Política Nacional de Inteligencia Artificial
N015	Resolución 1519	2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

Marco Normativo			
N016	Resolución 500	2021	Norma que establece la obligación de adoptar la estrategia de seguridad digital.
N017	Directiva Presidencial	2022	Refuerza la obligación de fortalecer la seguridad digital en las entidades públicas.

SITUACIÓN ACTUAL

La Empresa para la Seguridad y Soluciones Urbanas – ESU ha realizado actividades tendientes a la adopción del Modelo de Seguridad y Privacidad de la Información, para lo cual se tiene aprobada por la alta dirección de la ESU, la Política de Seguridad y Privacidad de la Información - V6, obteniendo los siguientes resultados:

Ámbito	Situación Actual
Diagnóstico de seguridad, Gobierno Digital y Privacidad de la Información	Se cuenta con un assessment de seguridad basado en el estándar internacional para la Seguridad de la Información ISO/IEC 27001:2022, la cual fue implementada de acuerdo con la Política de Seguridad y Privacidad de la Información en la ESU, vigencia 2024. Se tiene la participación de la alta dirección de la Empresa para la Seguridad y Soluciones Urbanas – ESU en la aprobación de la Política de Seguridad y Privacidad de la información ESU, la cual se encuentra publicada en el Sistema Integrado de Planeación y Gestión – KAWAK.
Plan de Seguridad, Gobierno Digital y Privacidad de la Información	En la vigencia 2025, se crea y formaliza el plan de seguridad, gobierno digital y privacidad de la información para las vigencias 2025-2027. Así mismo, se tiene actualizado dicho plan con las actividades realizadas durante la vigencia 2024 y se actualizaron las actividades a realizar para la vigencia 2025. Es necesario fortalecer los procesos y procedimientos que hacen referencia a la implementación de la seguridad y privacidad de la información en la ESU.

Ámbito	Situación Actual
	Se cuenta con la Aplicabilidad de la ESU en materia de seguridad y privacidad de la información, conforme a los controles de la norma ISO/IEC 27001:2022. Se cuenta en la ESU con un plan para recuperación ante desastres (DRP), para garantizar la restauración de las operaciones críticas de forma rápida y ordenada. Se elaboró, publicó y socializó la caracterización de la gestión de tecnología de la información, cuyo objetivo es gestionar de manera integral los servicios tecnológicos mediante el establecimiento de políticas, planes, programas y proyectos orientados al fortalecimiento estratégico y misional de la entidad.
Plan de Implementación	El plan de seguridad, gobierno digital y privacidad de la información se actualizará periódicamente con el fin de hacer seguimiento a las acciones definidas en cada vigencia y determinar las acciones a realizar en las siguientes vigencias. La identificación de riesgos e implementación de controles de Seguridad y Privacidad de la Información están alineados al procedimiento denominado "caracterización gestión de tecnología de información" liderado por la Oficina Estratégica.
Gestión de Riesgos	La Empresa para la Seguridad y Soluciones Urbanas – ESU ha implementado el manejo y respuesta a incidentes asociados a Seguridad y Privacidad de la Información, mediante la "caracterización gestión de tecnología de información".

Las principales actividades realizadas durante la vigencia 2024 se describen a continuación:

Eje	Área	Actividades Realizadas
Transformación Digital	Transferencia de información	Se identificaron riesgos de seguridad digital y se implementaron los controles

Eje	Área	Actividades Realizadas
		de seguridad necesarios para garantizar la seguridad digital y la protección de los datos personales en el marco de los acuerdos de intercambio de información de la entidad con otros actores.
Riesgos	Correo electrónico (phishing e ingeniería social, spam)	De acuerdo con los resultados del assessment realizado en el año 2024, se identificaron oportunidades de mejora en la gestión de la seguridad de la información. Con base en estos hallazgos, se llevaron a cabo diversas actividades orientadas a fortalecer los controles existentes, mitigar riesgos y mejorar el nivel general de seguridad de la entidad.
	Relacionados con el factor humano	Se brinda inducción a los funcionarios de la ESU sobre el uso adecuado y seguro del almacenamiento en la nube, haciendo énfasis en las buenas prácticas para proteger la información. Durante la capacitación, se les instruye sobre la creación de contraseñas seguras (mínimo 12 caracteres alfanuméricos) y la activación del doble factor de autenticación como mecanismos esenciales de seguridad.
	Infraestructura (equipos de seguridad y servidores)	Se llevó a cabo un assessment de seguridad en el año 2024 al firewall y a los servidores de la ESU. Con base en los hallazgos obtenidos, se implementaron medidas de hardening en la infraestructura tecnológica, siguiendo las mejores

Eje	Área	Actividades Realizadas
		prácticas recomendadas por la norma ISO/IEC 27001:2022.
Sensibilización	Inducción de funcionarios	Se brindó a los funcionarios una inducción integral sobre el funcionamiento del área de Tecnología de la Información (TI) de la entidad, en la cual se socializaron los procesos, políticas, portafolio de servicios y acuerdos de nivel de servicio (SLA), con el propósito de asegurar el conocimiento, la correcta aplicación de los lineamientos establecidos y la alineación con los objetivos institucionales. Adicionalmente, se compartieron buenas prácticas de ciberseguridad orientadas al uso adecuado del equipo de cómputo y del correo electrónico institucional, con el fin de fortalecer la cultura de seguridad digital dentro de la entidad.
	Divulgación de la documentación, controles y herramientas de ayuda del sistema de gestión de tecnología de la información	En la inducción de los funcionarios se socializa la documentación, controles y herramientas del sistema de gestión de tecnología de la información institucional.
	Continuidad de la plataforma tecnológica y de servicios	Desde el área de Tecnología de la Información (TI) se realizó la implementación de soluciones de detección y respuesta ante intrusos, tales como FortiEDR, FortiCabs, FortiMail y FortiZtna, así como en la incorporación de equipos de seguridad Fortinet con tecnología SD-WAN. Estas

Eje	Área	Actividades Realizadas
		soluciones fortalecen la seguridad y protegen la infraestructura tecnológica que soporta los servicios institucionales.
		Se realizó un diagnóstico, diseño e implementación del Plan de Continuidad de Negocio Institucional.
Sistema integrado de planeación y gestión	Gestión de la Documentación del Sistema de gestión de seguridad de la información	Se actualizó el documento de contexto de política de seguridad y privacidad de la información institucional.
		Se diseñaron estrategias y controles que permitan la implementación de las políticas de seguridad de la información en los procesos institucionales.
Seguridad operativa	Gestión de eventos e incidentes de seguridad	Gestionar, evaluar e implementar acciones de respuesta frente a eventos e incidentes de seguridad de la información.
	Seguridad de la documentación generada en los procesos	Elaboración de lineamientos y controles para mejorar la seguridad de los datos procesados en los procesos institucionales a través de los sistemas de información.
	Seguridad de Aplicaciones de procesamiento de información de las plataformas estratégicas	Ejecución del diseño e implementación de lineamientos y controles que mejoren los niveles de seguridad de los sistemas de información institucionales y las aplicaciones.
	Análisis de vulnerabilidades de plataforma tecnológica	Ejecución del análisis de vulnerabilidades sobre los componentes de infraestructura tecnológica y de servicios de la Entidad.
	Ingeniería social	Desarrollo de pruebas de ingeniería social para evaluar

Eje	Área	Actividades Realizadas
		el nivel de conciencia en seguridad de la información de los funcionarios, contratistas y colaboradores de la Entidad.

Lineamientos de las siguientes actividades

Las responsabilidades y actividades asociadas a los lineamientos establecidos se encuentran definidas en el plan de implementación del modelo de privacidad y seguridad de la información.

- **Servicios ciudadanos digitales:** se tiene 2 plataformas tecnológicas donde interactúa la ciudadanía que son; la página web y el Portal de Contratación.

1. Ciudadanos que usan la página web para crear PQRSD (Peticiones, Quejas, Reclamos, Sugerencias y Denuncias).

Categoría Lineamiento Pagina Web	Descripción
Accesibilidad	La web debe cumplir con algunas normas de accesibilidad digital para garantizar que los ciudadanos puedan interactuar con los contenidos.
Disponibilidad del canal PQRSD	Debe estar claramente visible y accesible en la parte superior o barra lateral de la página principal, permitiendo radicar peticiones, quejas, reclamos, sugerencias y denuncias, con trazabilidad en línea.
Respuesta oportuna	Integración con el sistema de gestión documental para garantizar cumplimiento de los términos de ley (Ley 1755 de 2015).
Interacción en línea	Permitir al ciudadano consultar el estado de sus solicitudes PQRSD, recibir respuestas electrónicas y dar retroalimentación en la página web a través del botón de seguimiento.
Contenido actualizado	Información institucional, normatividad, servicios y trámites deben estar al día. Debe realizarse una verificación mínima trimestral.
Seguridad de la información	Toda la información recolectada por formularios web debe manejarse conforme a la Ley 1581 de 2012 (protección de datos personales) y con cifrado HTTPS.
Transparencia activa	Publicar secciones de transparencia conforme a la Ley 1712 de 2014 (acceso a la información pública).
Medición de satisfacción	Incluir mecanismos de retroalimentación y encuestas para evaluar la experiencia de usuario y satisfacción del ciudadano.

2. Los proveedores que interactúan con la entidad a través del portal de contratación.

Categoría Lineamiento Portal de Contratación	Descripción
Transparencia y Acceso Público	Publicar toda la información relacionada con los procesos de contratación (pliegos, actas, contratos, resultados, un buscador por palabras clave y filtros por tipo de proceso, estado y fecha).
	Incluir mecanismos de búsqueda eficientes y filtros (tipo de proceso, entidad, estado, fechas).
Cumplimiento Normativo	Operar conforme a lo dispuesto en el Reglamento de Contratación de la ESU y cuando sea aplicable al Estatuto General de Contratación de la Administración Pública en Colombia y demás normas complementarias.
	Aplicar principios de contratación pública: publicidad, transparencia, economía, eficiencia y selección objetiva. Así como los principios de la función administrativa y de la gestión fiscal enunciados en los artículos 209 y 267 de la Constitución Política de Colombia.
Accesibilidad y Usabilidad	En el portal de contratación se encuentra el procedimiento para participar en los procesos de contratación.
Seguridad de la Información	Implementar acciones de ciberseguridad y protección de datos, incluyendo autenticación multifactor para usuarios internos y proveedores, así como mecanismos de trazabilidad de accesos.
Promoción de la Participación	Facilitar la participación de Mipymes, comunidades étnicas y proveedores internacionales.
	Proporcionar información clara sobre requisitos y procesos.
	Promover inclusión social y económica.
Documentación y Soporte	Disposición de manuales, guías e instructivos.
	Disponer de soporte técnico y atención al usuario para resolver inquietudes.

- **Datos y Gobierno Abierto:**

Categoría	Lineamiento	Descripción
Datos Abiertos	Publicación obligatoria	Las entidades deben publicar datos en el portal oficial: Portal de contratación ESU
	Principios FAIR	Los datos deben ser Findables, Accessible, Interoperable y Reusable (localizables, accesibles, interoperables y reutilizables).
	Calidad y estandarización	Aplicar estándares de calidad en los conjuntos de datos, según Resolución 1519 de 2020.

Categoría	Lineamiento	Descripción
	Fortalecimiento de capacidades	Capacitar equipos en apertura, calidad, uso y aprovechamiento de datos abiertos.
Gobierno Abierto	Transparencia	Garantizar acceso a la información pública mediante plataformas digitales.
	Participación ciudadana	Fomentar canales para que la ciudadanía participe en decisiones públicas (encuestas, foros, consultas y publicar los resultados de los mismos en la página web institucional).
	Colaboración	Promover el trabajo conjunto entre entidades del Estado y sociedad civil.
	Accesibilidad y usabilidad	Cumplir estándares de accesibilidad web definidos por la Resolución 1519 de 2020.
Seguridad Digital	Protección de datos	Garantizar que los datos abiertos no incluyan información sensible o datos personales, en cumplimiento con el Modelo de Seguridad y Privacidad de la Información (MSPI)
	Integración con gobierno digital	Alinear las estrategias de datos y gobierno abiertos con los objetivos del Plan de Gobierno Digital y el Plan Estratégico de Tecnologías de la Información-PETI.
	Supervisión y seguimiento	Verificar los mecanismos de la política de seguridad y privacidad de la información que permitan medir el impacto y cumplimiento de estos lineamientos.

- **Desarrollar e implementar un Plan de Gestión de Seguridad Digital basado en el ciclo PHVA**

Fase del ciclo PHVA	Lineamiento	Descripción
Planificar	Diagnóstico y análisis GAP (o análisis de brechas)	Evaluar el estado actual de la entidad en relación con el Modelo de Seguridad y Privacidad de la Información (MSPI).
	Identificación de activos de información e infraestructura crítica	Determinar los activos de información y la infraestructura crítica que requieren protección.
	Valoración de riesgos	Evaluar los riesgos asociados a los activos de información identificados.
	Plan de tratamiento de riesgos	Desarrollar estrategias para mitigar los riesgos identificados.

Fase del ciclo PHVA	Lineamiento	Descripción
Hacer	Implementación de controles	Aplicar las medidas de seguridad necesarias para mitigar los riesgos.
	Establecimiento de roles y responsabilidades	Definir claramente los roles y responsabilidades en la gestión de la seguridad digital.
Verificar	Seguimiento y medición	Monitorear y evaluar la eficacia de las medidas implementadas.
Actuar	Revisión por la dirección	Evaluar los resultados y tomar decisiones para mejorar el sistema de gestión de seguridad.
	Mejora continua	Implementar acciones correctivas y preventivas para mejorar la seguridad digital.

- **Protección de Infraestructuras Críticas de Información (CII)**

Categoría	Lineamiento
Identificación de Activos	Mantener actualizados los catálogos de sistemas de información, servicios, bases de datos, activos de información, infraestructura, flujos de información y artefactos, facilitando la identificación de activos críticos.
Evaluación de Riesgos	Realizar periódicamente una evaluación del riesgo de seguridad digital, contando con normas, políticas, procedimientos y recursos necesarios para gestionar efectivamente el riesgo.
Plan de Seguridad Digital	Desarrollar un plan de seguridad digital que contemple la protección de redes, infraestructuras críticas cibernéticas, servicios esenciales y sistemas de información en el ciberespacio.
Gestión de Incidentes	Establecer un procedimiento de gestión de incidentes de seguridad digital, incluyendo la creación de una bitácora, designación de responsables y reporte de incidentes graves al (Computer Security Incident Response Team) CSIRT Gobierno.
Capacitación y Sensibilización	Realizar campañas de sensibilización y capacitación en seguridad digital para todos los funcionarios, desarrollando procesos de formación especializada para las áreas a cargo de la seguridad digital.
Monitoreo y Respuesta	Implementar mecanismos de gestión y monitoreo que protejan la infraestructura de TI de amenazas físicas y digitales, incluyendo la gestión de copias de seguridad y protocolos de acceso remoto.
Interoperabilidad Segura	Implementar controles y procesos que habiliten la integración al servicio ciudadano digital de interoperabilidad de forma segura, cumpliendo con los lineamientos dados en el marco de la política de gobierno digital.

- **Seguimiento seguridad y gobierno digital:**

Categoría	Lineamiento	Descripción
Evaluaciones internas	Definición de indicadores de seguimiento	Establecer indicadores para evaluar el avance del PETI.
	Autodiagnóstico de seguridad	Aplicar el autodiagnóstico específico de seguridad digital conforme al Modelo de Seguridad y Privacidad de la Información -MSPI.
Reportes oficiales	Reporte en FURAG	Reportar el avance de implementación a través del Formato Único de Reporte de Avance de Gestión (FURAG).
Seguimiento	Proceso de autoevaluación anual de seguridad y gobierno digital	Realiza evaluación anual con enfoque de mejoramiento continuo, verificando avances frente al año anterior.
Estrategia de seguridad digital	Adopción obligatoria	Implementar una estrategia institucional de seguridad digital conforme al Modelo de Seguridad y Privacidad de la Información (MSPI).
	Gestión de riesgos	Asegurar la identificación y tratamiento de riesgos digitales en la estrategia.
Normatividad aplicable	Resolución 500 de 2021	Norma que establece la obligación de adoptar la estrategia de seguridad digital.
	Directiva Presidencial 02 de 2022	Refuerza la obligación de fortalecer la seguridad digital en las entidades públicas.

- **Reporte y gestión de incidentes**

Categoría	Lineamiento
Procedimiento de Gestión	Establecer un procedimiento documentado para la gestión de incidentes de seguridad digital, que incluya la identificación, clasificación, tratamiento, investigación y cierre de incidentes.
Bitácora de Incidentes	Crear y mantener una bitácora detallada que registre todas las actividades realizadas durante la gestión de cada incidente, incluyendo fechas, responsables y acciones tomadas.
Responsables de Gestión	Designar a un responsable de seguridad digital dentro de la entidad, quien liderará la gestión de incidentes y coordinará con el CSIRT Gobierno cuando sea necesario.
Reporte al CSIRT Gobierno	Reportar al equipo de respuesta ante incidentes de seguridad informática (CSIRT) Gobierno los incidentes catalogados como "Muy Grave" o "Grave" utilizando el formato establecido por el CSIRT, disponible en sus canales oficiales.

Categoría	Lineamiento
Comunicación de Incidentes Menores	Los incidentes catalogados como "Menos Grave" o "Menor" deben ser comunicados al CSIRT Gobierno una vez gestionados, para llevar un registro estadístico y conocer las tipologías de los incidentes.
Planes de Mejoramiento	Tras la investigación de cada incidente, desarrollar planes de mejoramiento basados en el análisis de causa raíz, supervisados por el responsable de gestión de sistemas de la información para garantizar su cumplimiento.
Indicadores de Gestión	Establecer indicadores para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información.
Etapas de Gestión de Incidentes	Incluir en la estrategia de seguridad digital las actividades correspondientes a las etapas de: prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje.

- **Esquema de autoevaluación**

Categoría	Lineamiento
Objetivo del Diagnóstico	Realizar un diagnóstico o análisis GAP (análisis de brechas) para identificar el estado actual de la entidad respecto a la adopción del MSPI (Medición de Seguridad y Privacidad de la Información), utilizando la herramienta de autodiagnóstico del MSPI.
Instrumento de Evaluación	Utilizar el "Instrumento de Evaluación MSPI (Medición de Seguridad y Privacidad de la Información)" para identificar de forma específica los controles implementados y faltantes, con el fin de establecer insumos fundamentales para la fase de planificación.
Frecuencia de Evaluación	Realizar el autodiagnóstico antes de iniciar la fase de planificación y actualizarlo posterior al término de la fase de evaluación de desempeño, para identificar los avances en la implementación del MSPI.
Entradas Recomendadas	Revisar aspectos internos como talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.
Salidas Esperadas	Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI (Medición de Seguridad y Privacidad de la Información) en toda la entidad y sus acciones de mejora.
Propósito del Esquema	Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la entidad, como punto de partida para la implementación del MSPI.

PLAN PARA LA IMPLEMENTACIÓN DEL MODELO DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta la política de seguridad y privacidad de la información aprobado por Empresa para la Seguridad y Soluciones Urbanas - ESU y el resultado del análisis del estado actual de la implementación de seguridad y privacidad de la información, se establece el siguiente plan para la implementación del Modelo de Seguridad y Privacidad de la Información:

Acción	Responsable	Plazo Estimado	Observaciones	Objetivo Estratégico Relacionado	Riesgo Asociado Mitigado	Indicador (Línea base / Meta)	Periodicidad de Seguimiento
Incluir explícitamente los componentes de Servicios Ciudadanos Digitales (SCD) en el Plan de Seguridad.	TI	1 mes	Alinear con Decreto 1008 de 2018.	Cumplir normativa y fortalecer servicios digitales.	Incumplimiento normativo y vulnerabilidad de servicios digitales.	% de componentes incluidos en el plan (0% / 100%)	Mensual
Articular el Plan de Seguridad con la estrategia de Datos y Gobierno Abierto.	TI y Planeación	6 meses	En cumplimiento de la Política de Gobierno Digital.	Promover transparencia y gobernanza digital.	Riesgo de opacidad institucional y bajo cumplimiento de política digital.	% de alineación entre planes (0% / 100%)	Semestral
Desarrollar e implementar un Plan de Gestión de Seguridad Digital basado en el ciclo PHVA.	TI	6 meses	Alineado al CONPES 3995 de 2020.	Mejorar la gestión y cultura de seguridad.	Falta de control sobre incidentes y brechas en mejora continua.	% de avance en implementación del plan PHVA (0% / 100%)	Semestral
Diseñar e incluir estrategias de protección de Infraestructuras Críticas de Información (CII).	TI	1 mes	Requerimiento CONPES 3995 de 2020.	Proteger activos críticos de información.	Ciberataques o indisponibilidad de servicios esenciales.	% de CII identificadas y protegidas (20% / 100%)	Mensual
Formalizar el proceso de reporte y gestión de incidentes de seguridad ante el CSIRT Gobierno.	TI	6 meses	Basado en lineamientos de MinTIC.	Fortalecer la respuesta ante incidentes.	Manejo inadecuado o tardío de incidentes de seguridad.	% de incidentes reportados conforme al protocolo (30% / 100%)	Semestral

Acción	Responsable	Plazo Estimado	Observaciones	Objetivo Estratégico Relacionado	Riesgo Asociado Mitigado	Indicador (Línea base / Meta)	Periodicidad de Seguimiento
Implementar el esquema de autoevaluación anual de Seguridad Digital conforme a MinTIC.	TI	Cada vigencia anual	Autoevaluación obligatoria para entidades públicas.	Cumplir normativa y evaluar capacidades institucionales.		% de cumplimiento del instrumento de autoevaluación (0% / 100%)	Anual
Definir métricas de madurez en seguridad y gobierno digital en los sistemas de seguimiento.	TI y Planeación	Cada vigencia anual	Enfocado a medición de avance institucional.	Medir desempeño y madurez en seguridad digital.		% de indicadores definidos e integrados en el sistema de seguimiento (0% / 100%)	Anual
Ejecutar actividades de formación anual en seguridad digital: talleres, simulacros de ciberataques, campañas de concientización.	TI y Talento Humano	Cada vigencia anual	En línea con la política de seguridad digital y cultura organizacional.	Fomentar cultura de seguridad y reducir riesgos humanos.	Riesgo de incidentes por error humano o desconocimiento.	% de servidores capacitados por vigencia (línea base: 40% / meta: 90%)	Anual
Definir lineamientos para la incorporación de la IA en la ESU	TI	2026-2027	En línea con la política nacional de inteligencia artificial del Conpes 4144	Fomentar el desarrollo y adopción de la IA	Riesgos con la privacidad de los datos, la generación de sesgos en la toma de decisiones automatizadas y la falta de claridad sobre la propiedad intelectual de los resultados generados	Definición de estrategias operativas y éticas	Anual

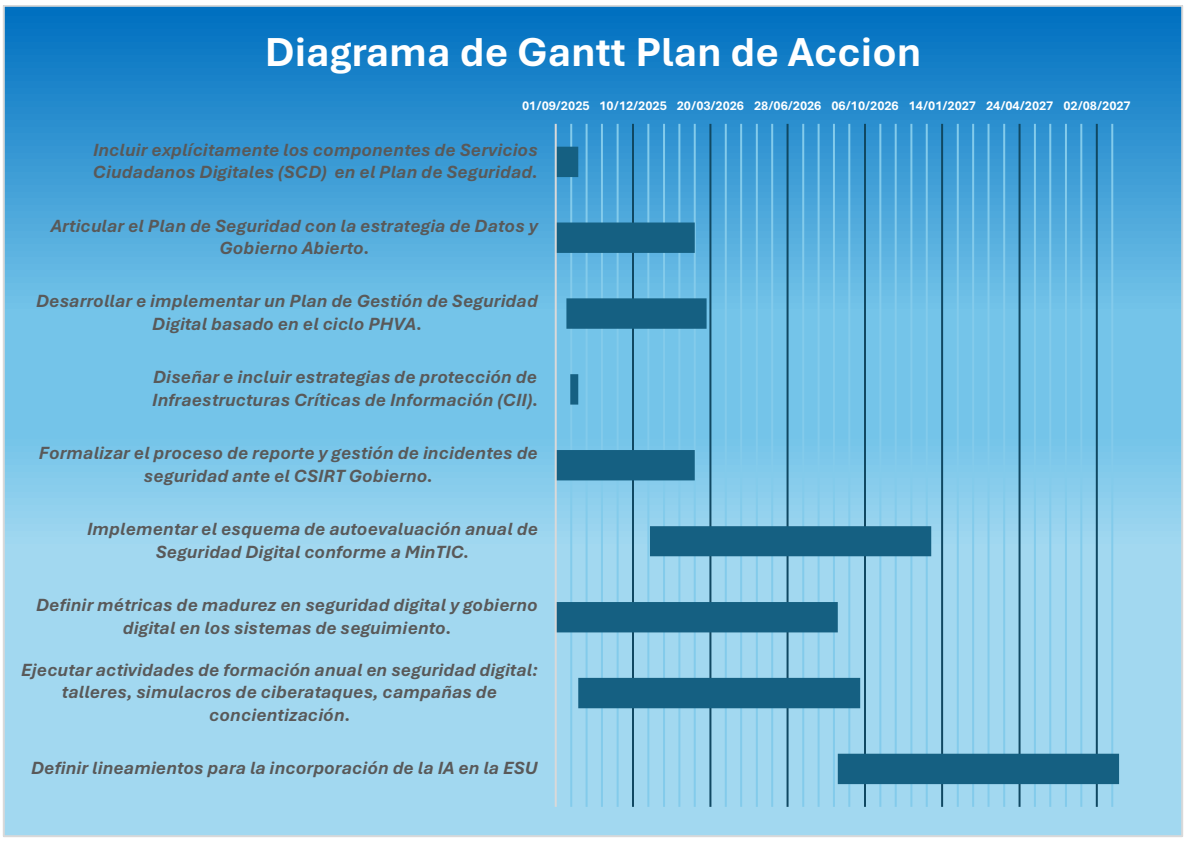
Diagrama de Gantt Plan de Accion
01/09/2025
10/12/2025
20/03/2026
28/06/2026
06/10/2026
14/01/2027
24/04/2027
02/08/2027
Incluir explícitamente los componentes de Servicios Ciudadanos Digitales (SCD) en el Plan de Seguridad.
Articular el Plan de Seguridad con la estrategia de Datos y Gobierno Abierto.
Desarrollar e implementar un Plan de Gestión de Seguridad Digital basado en el ciclo PHVA.
Diseñar e incluir estrategias de protección de Infraestructuras Críticas de Información (CII).
Formalizar el proceso de reporte y gestión de incidentes de seguridad ante el CSIRT Gobierno.
Implementar el esquema de autoevaluación anual de Seguridad Digital conforme a MinTIC.
Definir métricas de madurez en seguridad digital y gobierno digital en los sistemas de seguimiento.
Ejecutar actividades de formación anual en seguridad digital: talleres, simulacros de ciberataques, campañas de concientización.
Definir lineamientos para la incorporación de la IA en la ESU