INSTITUTO MINICIPAL DE CULTURA DE YUMBO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA 2025

ELABORACIÓN DEL DOCUMENTO DICIEMBRE DE 2024

EQUIPO COLABORADOR

GESTIÓN DE DIRECCIÓN Y PLANEACIÓN

MANTENIMIENTO Y ADMINISTRACIÓN DE BIENES

ENERO 31 DE 2025

JOHN SEBASTIÁN ECHEVERRY COLLAZOS
GERENTE

Reviso y aprobó: Comité de Gestión y Desempeño

Elaboró: Equipo de trabajo Planeación y Mantenimiento y Administración de Bienes.

CONTENIDO

1. INTRODUCCIÓN

El Instituto Municipal de Cultura de Yumbo -IMCY- (en adelante la *Entidad*), presenta el Plan de Seguridad y Privacidad de la Información (en adelante *PSPI*). El plan tiene como propósito cerrar brechas frente a la seguridad de la información organizacional interna y establecer medidas para ampliar la confianza digital al mejorar la seguridad digital de la Entidad

La información es el activo de mayor valor para la entidad, es un recurso vital y el buen uso puede significar la diferencia en el servicio, propendiendo por su éxito o fracaso.

El uso adecuado de la información es fundamental para lograr un alto nivel competitivo dentro del mercado y obtener mayores niveles de capacidad de desarrollo. Además, busca la solución de problemas y el crecimiento en conocimiento para apoyar la toma de decisiones, por ello, el MIPG considera el desarrollo del talento humano como trascendental para la gestión del conocimiento y las políticas de gobierno y seguridad digital con las TIC, como agente estratégico para la transformación digital y la competitividad de las entidades.

La gestión de la información facilita la previsión, prospección y oportunidad para la reacción, mantener control sobre las fortalezas y debilidades, así como amenazas y oportunidades, permitiendo proteger los activos más vulnerables como Entidad.

La seguridad de la información, por tanto, alcanza niveles de la misma relevancia, constituyendo un elemento fundamental para la protección efectiva de derechos, obligaciones y libertades del ciudadano. También, como componente transversal a la Estrategia de Gobierno Digital para la gestión, al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios, apoyando el tratamiento de la información utilizada en los trámitesy servicios que ofrece la Entidad, observando en todo momento las normas sobreprotección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información. Así las cosas y dada su importancia, la seguridad de la información es de carácter transversal a todas las áreas de la Entidad que, requiere el fortalecimiento del talento humano, procesos, tecnología en ámbitos de colaboración y participación, como elementos indispensables para reducir los factores que suponen un riesgo para la seguridad de la información.

2. OBJETIVO GENERAL

Fortalecer la Seguridad y Privacidad de la información de la entidad para garantizar la disponibilidad, confidencialidad e integridad de la información, mediante la aplicación de lineamientos y medidas que contribuyan a la seguridad de la información, la transparencia en la gestión pública y al incremento de la confianza ciudadana.

2.1 OBJETIVOS ESPECÍFICOS

1) Realizar copias de seguridad de la información
2) Respaldar copias de seguridad en sitio interno y externo de la entidad
3) Mantener actualizadas las aplicaciones de los sistemas de información
4) Gestionar riesgos de seguridad de la información
5) Controlar acceso a los sistemas de gestión de la información

3. ALCANCE

Fortalecer la seguridad de los procesos priorizados dados por los requisitos de las operaciones de negocio y los que se definan, interoperen y/o integren; para el cumplimiento de los objetivos institucionales.

4. NORMATIVIDAD

El presente Plan de Seguridad y Privacidad de la Información -PSPI-, soporta su revisión de normas concordantes y complementarias en el cumplimiento normativo aplicable a:

- Plan de acción de la entidad para la misma vigencia
- Decreto 612[1] del 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*".
- Artículo 2.2.22.3.14 del Decreto 1083 del 2015, Decreto Único Reglamentario del Sector de Función Pública que señala **Integración de los planes institucionales y estratégicos al Plan de Acción**. *"Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web,*

[1] Fuente: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=85742

a más tardar el 31 de enero de cada año".

(...)

11. Plan de Seguridad y Privacidad de la Información

(...)

- Artículo 74 de la Ley 1474 de 2011, *"Plan de acción de las entidades públicas".*

LEYES	
Ley 2294 del 2023	Por el cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia Potencia Mundial de la Vida".
Ley 1955 de 2019	Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pactopor Colombia, Pacto por la Equidad".
Ley 1978 de 2019	Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones.
Ley 1757 de 2015	Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática.
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.
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 otrasdisposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección dedatos personales.
Ley 19 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Ley 1474 de 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
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 yse dictan otras disposiciones.
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 informacióny de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otrasdisposiciones
Ley 1150 de 2007	Seguridad de la Información electrónica en contratación en línea
Ley 962 de 2005	Simplificación y racionalización de Tramite. Atributos de Seguridad de la Información electrónica de entidades publicas

DECRETOS	
Decreto 767 de 2022	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
Decreto 338 de 2022	Lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital
Decreto 88 de 2022	Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
Decreto 1287 de 2020	Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de servicios ciudadanos digitales
Decreto 2106 de 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en laadministración pública.
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.
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 lasentidades del Estado
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucionalen materia de tecnologías de la información y las Comunicaciones.
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 dela parte 2 del libro 2 del Decreto 1078 de 2015, Decreto ÚnicoReglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones y se dan Lineamientos Generales de la Estrategia de Gobierno en Línea.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictanotras disposiciones.

Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009y se dictan otras disposiciones
Decreto 333 de 2014	Define el régimen de acreditación de las entidades de certificación, aplicable a personas jurídicas, públicas y privadas
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 1510 de 2013	Por el cual se reglamenta el sistema de compras y contratación pública
Decreto 2693 de 2012	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otrasdisposiciones.
Decreto 2482 de 2012	Por el cual se establecen los lineamientos generales para la integración de la planeación y la gestión (Ley 489 de 1998, Ley 552 de1994).

DIRECTIVAS	
Directiva 26 de 2020	Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
Directiva 03 de 2019	Lineamientos para la definición de la estrategia institucional de comunicaciones, objetivos y contenidos de las entidades de la ramaejecutiva del orden nacional
Directiva 02 de 2000	Plan de Acción de la estrategia de Gobierno en Línea.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL	
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital
CONPES 3975 de 2019	Política Nacional de Transformación Digital e Inteligencia Artificial.
CONPES 3920 de 2018	Política Nacional de Explotación de Datos (BIG DATA)
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y ciberdefensa
CONPES 3292 de2004	Política Nacional Realización y Automatización de Tramites
CONPES 3248 de 2003	Renovación de la administración pública

RESOLUCIONES	
MINTIC, Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información (MSPI) y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
MINTIC, Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
MINTIC, Resolución 1519 de 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.
DAFP, Guía de 2020	Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas (Riesgos de Gestión, Corrupción y Seguridad Digital) Versión 5

5. RESPONSABILIDAD Y AUTORIDAD

La Autoridad del presente plan es el gerente de la Entidad o quién ejerza el rol de representante legal, y/o, a través de quién ejerce el rol del profesional apoyo al área de sistemas.

6. DEFINICIONES

Aplican las definiciones contenidas en el “Glosario” referido en el capítulo 5. del Modelo Nacional de Seguridad y Privacidad de la Información – MSPI-, que puede ser consultado en el siguiente enlace:

www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

7. DESARROLLO

7.1 INTERACCIÓN MODELOS MSPI y MGRSD

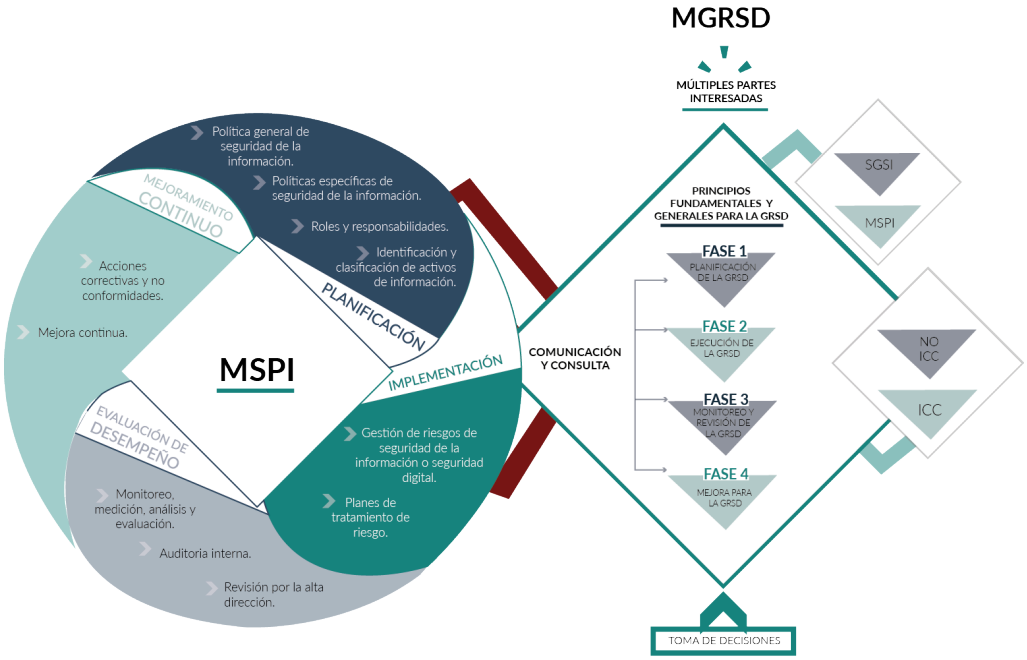
El Plan de Seguridad y Privacidad de la Información se basa en dos modelos a saber; Por un lado, en el Modelo de Seguridad y Privacidad de la Información (MSPI) e implementando el Sistema de Gestión de Seguridad de la Información (SGSI). Y por otro lado, en el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSI).

El Modelo de Seguridad y Privacidad de la Información (MSPI) se compone de las fases de diagnóstico, planeación, implementación, verificación y actuar, y a través de la implementación del Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión de Seguridad de la Información (SGSI) contempla grandes conjunto de actividades dentro de cada una de las fases como son: Diagnóstico inicial del estado del sistema con el fin de validar la brecha y las acciones que se deben desarrollar para su mitigación, actualización o elaboración de la documentación, sensibilización y capacitación, identificación y clasificación de los activos de información, identificación, valoración y gestión y tratamiento del riesgo de seguridad digital, revisiones del sistema, auditorías internas y externas, implementación de controles técnicos, entre otras.

El Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), abarca el monitoreo, revisión y mejora para las actividades propias de la gestión de riesgos de seguridad digital.[2]

Ilustración 1: Interacción Modelos MSPI y MGRSD



Fuente: MinTIC

[2] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

7.2 SITUACION ACTUAL DE LA ENTIDAD

La Seguridad y Privacidad de la Información se mantiene con las acciones concebidas por la Gestión de operaciones TI en la Entidad por parte del área de sistemas.

Desde el alcance de la operación actual, se avanza con acciones que, progresivamente van cerrando brechas de seguridad digital.

7.2.1 CIBERSEGURIDAD DE LA INFRAESTRUCTURA TI

La entidad dispone de una Infraestructura de Tecnologías de Información (TI) On-Premise (Local) situada en su sede principal.

La ciberseguridad sobre la Infraestructura TI, está apoyada con herramientas y acciones de ciberdefensa a saber:

Por un lado, en la Seguridad de la Red de datos se emplea Firewall para la seguridad perimetral, Antivirus para la seguridad de puntos finales y autenticación de usuarios autorizados con atributos de permisos para tener acceso a los servicios de red y aplicaciones.

Por otro lado, la Seguridad Física en el centro de datos y centros de cableado están provistos con equipos tecnológicos entre ellos; cámaras de video vigilancia, UPS para el suministro de energía eléctrica regulada y sistema de refrigeración.

Y, de otra parte, la Seguridad en la Nube aquella proporcionada por los proveedores tecnológicos con los que se tienen servicios contratados.

8. ACTIVIDADES DEL PLAN

A continuación, las actividades definidas para el Plan de seguridad y privacidad de la información.

El avance estará supeditado al apalancamiento y la capacidad institucional, ante lo cual se revisará la priorización y su implementación procederá acorde con las necesidades institucionales bajo principios de gradualidad, proporcionalidad y disponibilidad de recursos específicos.

ID	Actividad	Responsables	Fecha
1	Actualizar el diagnóstico de seguridad y privacidad de la información	Líderes de procesos, Área de sistemas.	Recurrente, cada año
2	Actualizar procedimientos e instructivos asociados a la seguridad y privacidad de la información	Área de sistemas	2025
3	Actualizar el Inventario de activos de información	Líderes de procesos, Área de sistemas.	2025
4	Socializar a los colaboradores de la entidad, los lineamientos establecidos de seguridad y privacidad de la información	Líderes de procesos, Área de sistemas.	2025
5	Revisar los controles propuestos por las dependencias, para mitigar los riesgos de seguridad de la información identificados.	Líderes de procesos, Área de sistemas.	2025
6	Concertar mesas de trabajo con los líderes de proceso, para categorizar los tratamientos del riesgo propuestos en sus mapas de proceso.	Líderes de procesos, Área de sistemas.	2025
7	Mejorar la ciberseguridad de la Infraestructura TI	Área de sistemas	2025

9. PLAN DE COMUNICACIONES

El presente plan será socializado a la comunidad e interesados, mediante publicación en el sitio web de la entidad: www.imcy.gov.co

10. EVALUACIÓN

La evaluación del presente plan se realizará de acuerdo con las acciones establecidas dentro del mismo y con base en ellas se realizarán las mejoras necesarias para cumplir con el ciclo PHVA.

JOHN SEBASTIÁN ECHEVERRI COLLAZOS
GERENTE

Revisó y aprobó. John Sebastián Echeverri C. - Gerente
Elaboró. Hyulder Echeverri Castro.
Original: Archivo de gestión IMCY