****

**PLAN DE SEGURIDAD Y**

**PRIVACIDAD DE LA**

**INFORMACIÓN**

***UAESP***

***Enero 2025***

**CONTENIDO**

[TÉRMINOS Y DEFINICIONES 3](#_Toc186797183)

[1. INTRODUCCIÓN 5](#_Toc186797184)

[2. OBJETIVO 6](#_Toc186797185)

[2.1 Objetivos Específicos 6](#_Toc186797186)

[3. REFERENCIA NORMATIVA 7](#_Toc186797187)

[4. RESPONSABLES DE LA IMPLEMENTACIÓN 8](#_Toc186797188)

[5. ALCANCE 10](#_Toc186797189)

[6. ANÁLISIS DE BRECHA 10](#_Toc186797190)

[7. ESTRATEGIA DE SEGURIDAD DIGITAL E IMPLEMENTACIÓN DEL MSPI 11](#_Toc186797191)

[8. VERIFICACIÓN 16](#_Toc186797199)

[9. REVISIÓN Y ACTUALIZACIÓN 17](#_Toc186797200)

[10. APROBACIÓN 17](#_Toc186797201)

 **ÍNDICE DE FIGURAS**

[Figura 1 Autodiagnóstico MSPI noviembre 2025 11](#_Toc185402257)

**ÍNDICE DE TABLAS**

[Tabla 1 Hoja de ruta 11](#_Toc156308327)

# TÉRMINOS Y DEFINICIONES

**Activos de información**: Toda información o elemento relacionado con el tratamiento de esta (Documentos, hardware, software, servicios, edificios, personas, entre otros) que tenga valor para la organización y por lo tanto se debe proteger. Se puede considerar un activo de información los datos creados o utilizados por un proceso, pueden ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, equipos de cómputo relacionados al tratamiento o almacenamiento de información, software del sistema, servicios utilizados para la transmisión, recepción y control de la información, entre otros.

**Administración de Riesgos:** Conjunto de elementos de control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.

**Amenaza**: Causa potencial de un incidente no deseado que puede provocar daños o afectaciones aun activo de información.

**Autoridad competente**: Es la autoridad apta e idónea para tratar de un determinado procedimiento o proceso de acuerdo con la ley.

**Ciberseguridad:** protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa almacena y transporta mediante los servicios de información que se encuentran interconectados.

**Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO 27000].

**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

**Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3)

**Disponibilidad**: La propiedad de tener la información cuando es requerida. Se relaciona con la facilidad y oportunidad de acceso a la información.

**Evaluación del Riesgo:** Permite comparar los resultados de su calificación, con los
criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos ubicados en los niveles: Nivel bajo,
moderado, alto y extremo y fijar prioridades de las acciones requeridas para su
tratamiento.

**Evento de seguridad de la información**: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la Política de Seguridad de la Información o falla en los controles.

**Incidente de seguridad de la información**: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la Entidad y de amenazar la seguridad y privacidad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

**Integridad**: Propiedad de la información relativa a su exactitud y completitud. [ISO 27000].

**MSPI**: Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MinTIC.

**Partes Interesadas:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

**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. (ISO/IEC 27000).

**Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Es pertinente señalar que "seguridad de la información" no solo corresponde a Seguridad Informática, sino que su alcance se complementa con ciberseguridad, seguridad física, ambiental y del recurso humano entre otras, buscando mantener la confidencialidad, la disponibilidad e integridad de la información. [Directiva 002 de 2021 – Alcaldía Mayor de Bogotá].

**Seguridad digital**: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

**SGSI**: Sistema de Gestión de la Seguridad de la Información.

**Sistema de información**: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

**Tratamiento**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

**Usuario**: Cualquier persona que tiene acceso a la plataforma y a los activos de información, sea en calidad de usuario final, tercero o administrador de la plataforma.

**Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

# INTRODUCCIÓN

En la era actual de creciente digitalización, la Unidad Administrativa Especial de Servicios Públicos reconoce la necesidad imperante de establecer un sólido plan de seguridad y privacidad. Este documento no solo sirve como una hoja de ruta estratégica, sino como una guía para la implementación y mantenimiento efectivo del modelo de seguridad y privacidad de la información -MSPI- definido por el Ministerio de Tecnologías de la Información y Comunicaciones MinTIC.

Este documento aborda los procesos y acciones concretas necesarios para asegurar la confidencialidad, integridad y disponibilidad de los activos críticos administrados por la UAESP. La hoja de ruta se concentra en acciones operativas, procedimientos prácticos y la promoción de una cultura interna de concientización para fortalecer la resiliencia ante las amenazas emergentes en el ámbito de la seguridad y privacidad. Al seguir este plan, la Unidad Administrativa Especial de Servicios Públicos no solo protegerá activamente la información sensible, sino que también consolidará la confianza de los ciudadanos en nuestra capacidad para salvaguardar sus intereses.

# OBJETIVO

Fortalecer la seguridad y privacidad de la información en la Entidad mediante la optimización del Modelo de Seguridad y Privacidad de la Información (MSPI), incrementando el nivel de madurez y el porcentaje de cumplimiento de los controles establecidos, en alineación con los lineamientos del habilitador de seguridad de la información de la Política Nacional de Gobierno Digital, con el propósito de garantizar la confidencialidad, integridad, disponibilidad y protección de los datos personales, así como la resiliencia ante riesgos tecnológicos y cibernéticos.

## 2.1 Objetivos Específicos

* Verificar y evaluar el cumplimiento de los requisitos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la aplicación del instrumento de evaluación proporcionado por el MinTIC.
* Diseñar e implementar acciones correctivas y de mejora continua que fortalezcan la eficacia del MSPI y lo adapten a las necesidades específicas de la Entidad.
* Incrementar el porcentaje de implementación de controles del MSPI, para aumentar el nivel de madurez del modelo de "Gestionado" a "Optimizado", en cumplimiento de los estándares y lineamientos definidos”

# REFERENCIA NORMATIVA

* CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital.
* Decreto 103 de 2015 el cual reglamenta la ley 1712 de 2014 ley de transparencia y del derecho de acceso a la información pública nacional.
* Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, “Protección de datos personales”.
* Ley 1712 del 6 de marzo de 2012 Por medio de la cual se crea la Ley de Transparencia y del Derecho al Acceso a la Información Pública Nacional, y se dictan otras disposiciones
* Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.
* Decreto 1083 del 26 de mayo de 2015, artículo 2.2.22.3.14 Por el cual se expide el Decreto Único Reglamentario del Sector Función Pública, y se compila, entre otros, los Decretos: 1499 de 2017: Sistema de Gestión establecido en el Artículo 133 de la Ley 1753 de 2015; 612 de 2018: Integración de los planes institucionales y estratégicos al plan de acción.
* ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de Información.
* Resolución No. 757 de 2023: Por la cual se adopta el Sistema de Gestión en la Unidad Administrativa Especial de Servicios Públicos UAESP y se derogan la Resoluciones 313 de 2020 y 571 de 2021.
* Decreto 767 de 2022: "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 338 de 2022 Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
* 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 seguridad y privacidad de la información y el manual de políticas de seguridad de la información.
* 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.

# RESPONSABLES DE LA IMPLEMENTACIÓN

Se adopta al interior de la Entidad la Resolución 757 de 2023 “Por la cual se adopta el Sistema de Gestión en la Unidad Administrativa Especial de Servicios Públicos UAESP y se derogan la Resoluciones 313 de 2020 y 571 de 2021"”.

Artículo 2° CREACIÓN DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO DE LA UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS. Créase el Comité Institucional de Gestión y Desempeño en la Unidad Administrativa Especial de Servicios Públicos (UAESP), encargado de orientar la implementación y seguimiento del Sistema de Gestión y la operación del MIPG, articulando todos los procesos y actividades de la UAESP, recursos, herramientas, estrategias y políticas de gestión y desempeño institucional, de acuerdo con la normatividad vigente en la materia.

Artículo 32°. MESAS TÉCNICAS DE TRABAJO. Con el fin de garantizar el óptimo funcionamiento del Comité Institucional de Gestión y Desempeño, del Comité Institucional de Coordinación de Control Interno de la UAESP y el de facilitar la implementación y desarrollo del Modelo Integrado de Planeación y Gestión, se podrán conformar mesas técnicas de trabajo necesarias para operacionalizar las Políticas del MIPG vigentes en la UAESP en la entidad, cuando el desarrollo de la respectiva política requiera la articulación de dos o más procesos o dependencias.

Por lo anterior, y de acuerdo con las funciones descritas del Comité Institucional de gestión y Desempeño en el artículo 4, es responsabilidad de la Dirección velar por la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- mediante el aseguramiento de la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad y privacidad de la información.

Así mismo, la Oficina TIC como líder de la Política de Seguridad Digital, a través de la mesa técnica de Seguridad Digital hará seguimiento a la Implementación del Modelo de Seguridad y Privacidad de Información – MSPI en la Entidad.

# ALCANCE

Este plan aplica a todos los procesos de la UAESP, en alineación con el alcance definido para el Sistema de Gestión de Seguridad de la Información (SGSI), que a su vez está integrado dentro del Sistema Integrado de Gestión (SIG) de la Entidad, garantizando la implementación y seguimiento de prácticas que promuevan la seguridad y privacidad de la información en todos los niveles organizacionales.

# ANÁLISIS DE BRECHA

La Entidad utiliza la herramienta diseñada por el MinTIC para realizar autoevaluaciones periódicas del nivel de implementación y madurez del Modelo de Seguridad y Privacidad de la Información (MSPI). Adicionalmente, las evaluaciones realizadas por la Oficina de Control Interno en noviembre de 2024 proporcionaron una perspectiva integral sobre el estado actual del modelo. Estas evaluaciones han permitido identificar brechas existentes en la implementación, las cuales servirán como base para definir una hoja de ruta clara y las acciones necesarias para alcanzar las metas establecidas por el MinTIC en el Decreto 1078 de 2015.

Figura 1 Autodiagnóstico MSPI noviembre 2025



Fuente: Propia

En la última auditoría del MSPI, se obtuvo una calificación cuantitativa promedio del 79% en controles implementados. Esto indica una implementación significativa, pero aún insuficiente para alcanzar el nivel de madurez “Optimizado”. Por lo tanto, el presente plan tiene como objetivo principal llevar a la Entidad a un nivel de madurez “Optimizado” mediante la implementación de los controles administrativos técnicos y operativos por encima del 80% de los controles definidos en el MSPI de acuerdo con los recursos de la Entidad.

# ESTRATEGIA DE SEGURIDAD DIGITAL E IMPLEMENTACIÓN DEL MSPI

De acuerdo con el análisis de la brecha encontrada del MSPI implementado en la Entidad, así como en las Políticas de Seguridad y Privacidad de la Información y las acciones definidas en el plan de mejoramiento del proceso de gestión tecnológica y de la información, se proponen las siguientes actividades para potenciar los niveles de madurez y los controles establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), integrando de manera efectiva la Estrategia de Seguridad Digital:

Tabla 1 Hoja de ruta

| **DOMINIO** | **#** | **ACTIVIDADES** | **ENTREGABLE** | **RESPONSABLE** | **FECHA** |
| --- | --- | --- | --- | --- | --- |
| **Política de seguridad de la información (A.1)** |  | Actualizar las políticas de seguridad y privacidad de la información. | Políticas actualizadas y aprobadas. | Oficina TIC | 30/05/2025 |
|  | Realizar autodiagnóstico MSPI. | Acta del comité institucional de gestión y desempeño. | Oficina TIC | 31/07/2025 |
| **Organización de la seguridad de la información (A.2)** |  | Reforzar los lineamientos de seguridad en la gestión de proyectos en la Entidad. | Comunicado Oficial para el cumplimiento de la resolución 648 del 2023 o aquella que la sustituya o haga sus veces. | Oficina TIC | 30/06/2025 |
|  | Documentar las matrices de roles y perfiles para los sistemas o aplicativos críticos de la Entidad. | Matrices de perfiles o documento equivalente. | Oficina TIC | 30/06/2025 |
| **Gestión de Activos (A.4)** |  | Revisar el procedimiento o lineamientos para el etiquetado de activos de información | Procedimiento o lineamientos actualizados. | Oficina TIC | 30/04/2025 |
|  | Socializar los lineamientos para el inventario de activos de información, focalizando en el Registros de Activos e Índice de información clasificada y reservada | Listado de Asistencia. | OTIC | 31/05/2025 |
|  | Realizar la actualización del inventario de activos de información. | Inventario de activos de información aprobado por la Dirección. | Todos los procesos | 31/07/2025 |
|  | Seguimiento al etiquetado de activos de información. | Oficio de solicitud de etiquetado de activos de información | Oficina TIC | 30/08/2025 |
| **Continuidad del Negocio (A.5)** |  | Actualizar el plan de pruebas de continuidad del negocio que incluya todos los procesos. | Plan de Continuidad del Negocio Actualizado. | Oficina Asesora de Planeación. | 31/12/2025 |
| **Cumplimiento (A.6)** |  | Elaborar el plan de pruebas de penetración 2025. | Plan Aprobado por el Comité Institucional de Gestión y Desempeño | Oficina TIC | 31/05/2025 |
|  | Realizar auditoria al MSPI | Informe de Auditoría al MSPI | OCI | 31/12/2025 |
| **Control de Acceso (T.1)** |  | Verificar el funcionamiento de las GPO y configuraciones necesarias en relación con la solicitud de cambio de contraseñas la primera vez de uso y el cambio periódico de acuerdo con las políticas de seguridad definidas en la entidad. | Informe de funcionamiento de las GPO | Oficina TIC | 31/12/2025 |
|  | Revisar la pertinencia de crear un procedimiento para la gestión de códigos fuentes de acuerdo con el control. | Procedimiento o Acta de reunión con la revisión de la pertinencia. | Oficina TIC | 31/12/2025 |
| **Criptografía (T.2)** |  | Realizar sensibilización sobre phishing e ingeniería social. | Listado de asistencia. | Oficina TIC | 31/07/2025 |
|  | Revisar e implementar solución para la gestión de secretos o claves | Informe de solución o servicio para gestión de llaves y secretos. | Oficina TIC | 31/07/2025 |
| **Seguridad en las Operaciones (T.4)** |  | Definir e implementar plan de respaldos y pruebas de restauración. | Informe de pruebas de restauración. | OTIC | 31/12/2025 |
| **Seguridad en los procesos de desarrollo y soporte** |  | Pruebas de seguridad para desarrollos antes de salida a producción durante la vigencia 2025. | Informe | OTIC | 31/12/2025 |
| **Gestión de incidentes de seguridad de la información (T.7)** |  | Revisión de la pertinencia de actualizar el procedimiento gestión de incidentes y el protocolo de respuesta de ser necesario. | Procedimiento actualizado o acta de reunión de pertenencia del procedimiento. | Oficina TIC | 31/12/2025 |
|  | Solicitar a proveedores o concesionarios reporte de incidentes de seguridad de la información en relación con los activos de información que son de responsabilidad de la UAESP. | Reporte de concesionarios | Procesos Misionales | 31/12/2025 |

Fuente: Elaboración Propia

Como parte integral de la estrategia de seguridad digital, este plan se articula con el Plan de Tratamiento de Riesgos, así como con otros planes de mejoramiento y estrategias previamente documentadas por la Entidad. Estas acciones buscan cerrar las brechas identificadas y consolidar un enfoque integral que fortalezca la resiliencia y eficacia del Modelo de Seguridad y Privacidad de la Información (MSPI). De esta manera, se promueve una gestión holística de la seguridad y privacidad de la información, en alineación con los objetivos estratégicos, normativos y el entorno digital de la organización.

1.
2.
3.
4.
5.
6.
7.

# VERIFICACIÓN

La verificación del cumplimiento del plan se realizará a través del indicador “Ejecución del Plan de Seguridad y Privacidad de la Información”:

$$Cumplimiento del PSPI=\frac{Actividades Ejecutadas}{Actividades Planeadas} ×100\%$$

De igual forma, el Oficial de seguridad de la información en conjunto con la OTIC podrán realizar autoevaluaciones que consideren necesarias al Modelo de Seguridad y Privacidad de la Información implementado, por medio de la herramienta definida por el MinTIC, para verificar el estado actual y realizar los ajustes pertinentes al plan de acción o por medio de los instrumentos de planes de mejoramiento definidos en la Entidad.

# REVISIÓN Y ACTUALIZACIÓN

El presente plan será revisado y actualizado al menos una vez al año o con mayor frecuencia, según lo requieran los lineamientos normativos o los cambios en el contexto interno o externo de la UAESP. Todas las actualizaciones deberán ser aprobadas por el comité institucional de gestión y desempeño para garantizar su alineación con los objetivos estratégicos de la Entidad.

# APROBACIÓN

|  |  |
| --- | --- |
| **Elaboró** | Juan Sebastián Perdomo Méndez – Profesional Universitario OTIC |
| **Revisó** | Jorge Alexis Rodriguez Meza – Jefe Oficina TICMesa Técnica de Seguridad Digital – Acta de reunión 18/12/2024 |
| **Aprobó** | Comité Institucional de Gestión y Desempeño – Acta de reunión xx/01/2025 |

