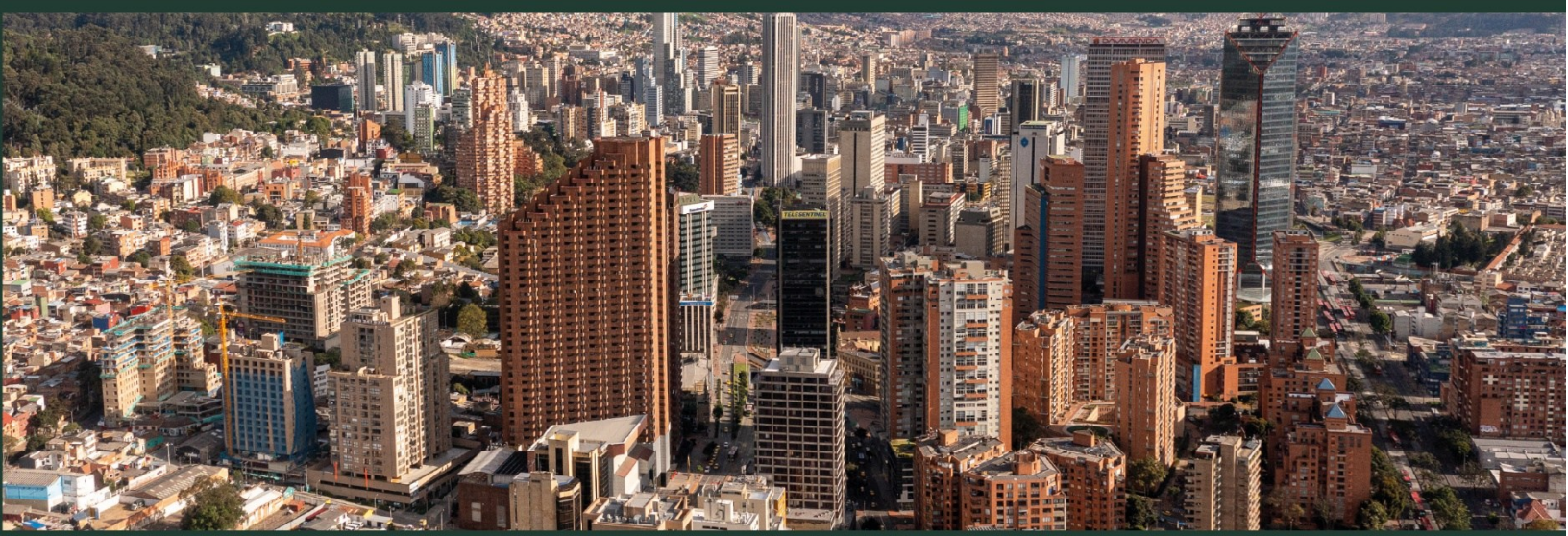




PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

Unidad Administrativa Especial de Servicios Públicos UAESP

Enero de 2026



UAESP



CONTENIDO

INDICE DE TABLAS	2
Tabla 1 Hoja de ruta	2
1. INTRODUCCIÓN	3
2. OBJETIVOS	3
2.1 Objetivos Específicos	3
3. ALCANCE	4
4. TERMINOS Y DEFINICIONES	4
5. REFERENCIA NORMATIVA	7
6. RESPONSABLES DE LA IMPLEMENTACIÓN	8
7. CIERRE EVALUACIÓN MSPI BAJO LA ISO: 27001:2013	9
8. ANÁLISIS DE BRECHA	11
9. ESTRATEGIA DE SEGURIDAD DIGITAL E IMPLEMENTACIÓN DEL MSPI	12
10. VERIFICACIÓN	25
11. REVISIÓN Y ACTUALIZACIÓN	26
12. APROBACIÓN	26

INDICE DE TABLAS

TABLA 1 HOJA DE RUTA	12
----------------------------	----

1. INTRODUCCIÓN

En la era actual de creciente digitalización, la Unidad Administrativa Especial de Servicios Públicos reconoce la necesidad imperante de establecer un 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.

2. OBJETIVOS

Planear las actividades establecidas en el Modelo Seguridad y Privacidad de la información (MSPI) que permitan aumentar el nivel de madurez y porcentaje de cumplimiento de los controles de seguridad y privacidad de la información con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la UAESP.

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”.

3. ALCANCE

Aplica a todos los procesos de la UAESP, alineado con el alcance definido para el Sistema de Gestión de Seguridad de la Información (SGSI), el cual 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.

4. TERMINOS 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).

5. REFERENCIA NORMATIVA

- **Constitución Política de Colombia – Nacional – 4 de julio de 1991** – Marco superior (derechos de privacidad, acceso a información pública).
- **Ley 1581 de 2012 – Nacional – 17 de octubre de 2012** – Protección de datos personales.
- **Ley 1712 de 2014 – Nacional – 6 de marzo de 2014** – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- **Decreto Nacional 1377 de 2013 – Nacional – 27 de junio de 2013** – Reglamenta parcialmente la Ley 1581 de 2012 (protección de datos).
- **Decreto Nacional 103 de 2015 – Nacional – 20 de enero de 2015** – Reglamenta la Ley 1712 de 2014 (gestión de información pública).
- **Decreto Nacional 1081 de 2015 – Nacional – 26 de mayo de 2015** – Decreto Único Reglamentario del Sector Presidencia (incluye disposiciones relacionadas con transparencia/acceso a información).
- **Decreto Único Reglamentario 1078 de 2015 (MinTIC) – Nacional – 26 de mayo de 2015** – DUR del sector TIC (base normativa de Gobierno Digital y lineamientos asociados a seguridad y privacidad/MSPI).
- **Decreto Único Reglamentario 1083 de 2015 (Función Pública) – Nacional – 26 de mayo de 2015** – DUR del sector Función Pública (incluye disposiciones del Sistema de Gestión/MIPG).
- **Decreto Nacional 1499 de 2017 – Nacional – 11 de septiembre de 2017** – Modifica el Decreto 1083 de 2015 en lo relacionado con MIPG.

- **Decreto Nacional 612 de 2018 – Nacional – 4 de abril de 2018** – Integración de planes institucionales y estratégicos al plan de acción.
- **Decreto Nacional 338 de 2022 – Nacional – 8 de marzo de 2022** – Fortalece la gobernanza de seguridad digital (adiciona Título 21 al DUR 1078 de 2015).
- **Decreto Nacional 767 de 2022 – Nacional – 16 de mayo de 2022** – Lineamientos generales de la Política de Gobierno Digital (ajusta/subroga partes del DUR 1078 de 2015).
- **Resolución MinTIC 1519 de 2020 – Nacional – 24 de agosto de 2020** – Estándares para publicar información Ley 1712; accesibilidad web, seguridad digital y datos abiertos.
- **Resolución MinTIC 500 de 2021 – Nacional – 10 de marzo de 2021** – Lineamientos/estándares de seguridad digital y adopta el MSPI.
- **Resolución MinTIC 746 de 2022 – Nacional – 11 de marzo de 2022** – Fortalece el MSPI y define lineamientos adicionales (respecto a la 500 de 2021).
- **Resolución MinTIC 02277 de 2025 – Nacional – 3 de junio de 2025** – Actualiza el Anexo 1 de la Resolución 500 de 2021 y deroga otras disposiciones
- **Resolución UAESP 757 de 2023 – Interna (Entidad Distrital) – 25 de septiembre de 2023** – Adopta el Sistema de Gestión en la UAESP y deroga Resoluciones 313 de 2020 y 571 de 2021.
- **Documento CONPES 3995 de 2020 – Nacional – 1 de julio de 2020** – Política Nacional de Confianza y Seguridad Digital.
- **ISO/IEC 27000:2013 – Internacional – (año 2013)** – Familia 27000 (referencia general).
- **ISO/IEC 27000:2022 – Internacional – (año 2022)** – Seguridad de la información/ciberseguridad y privacidad (familia 27000).

6. RESPONSABLES DE LA IMPLEMENTACIÓN

Se adopta al interior de la Entidad la Resolución 757 de 2023 “Por la cual se incorpora 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” en la cual se define que:

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 Gobierno y Seguridad Digital hará seguimiento a la Implementación del Modelo de Seguridad y Privacidad de Información – MSPI en la Entidad.

7. CIERRE EVALUACIÓN MSPI BAJO LA ISO: 27001:2013

Con la actualización de la norma ISO 27001 a su versión 2022, la Oficina de Control Interno (OCI) realizó la auditoría al MSPI con radicado No. 20251100092743 del 28/11/2025, verificando el cumplimiento y el avance de las acciones tomadas por la OTIC.

Los resultados mostraron un cumplimiento del 83%, frente al 79% registrado en la auditoría de 2024, lo que representa una mejora del 4%. Esta mejora se atribuye al cierre oportuno de las observaciones y a la ejecución de las acciones de mejora por parte de la OTIC.

Con base al informe de auditoría de la OCI, la evaluación bajo ISO 27001:2013 queda cerrada con un nivel de efectividad optimizado, como se detalla a continuación:

FIGURA 1 - EVALUACIÓN CIERRE MSPI - ISO:27001-2013

DOMINIO	Calificación Seguimiento OCI_noviembre 2025	Calificación Seguimiento OCI_noviembre 2024	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2025	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2024
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO	100	OPTIMIZADO
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	86	82	OPTIMIZADO	100	OPTIMIZADO
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO	100	OPTIMIZADO
A.8 GESTIÓN DE ACTIVOS	87	81	OPTIMIZADO	100	OPTIMIZADO
A.9 CONTROL DE ACCESO	75	70	GESTIONADO	100	GESTIONADO
A.10 CRIPTOGRAFÍA	70	70	GESTIONADO	100	GESTIONADO
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	85	83	OPTIMIZADO	100	OPTIMIZADO
A.12 SEGURIDAD DE LAS OPERACIONES	81	77	OPTIMIZADO	100	GESTIONADO
A.13 SEGURIDAD DE LAS COMUNICACIONES	77	74	GESTIONADO	100	GESTIONADO
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	86	86	OPTIMIZADO	100	OPTIMIZADO
A.15 RELACIONES CON LOS PROVEEDORES	80	80	GESTIONADO	100	GESTIONADO
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	80	GESTIONADO	100	GESTIONADO
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	50	GESTIONADO	100	GESTIONADO
A.18 CUMPLIMIENTO	87	79	OPTIMIZADO	100	GESTIONADO
CIERRE DE MSPI CON NORMA ISO/IEC 27001:2013	83	79	OPTIMIZADO	100	GESTIONADO
Nota: Esta calificación se generó con las acciones realizadas sobre observaciones y recomendaciones por el proceso a la evaluación del período anterior. Con lo cual se da cierre a esta evaluación bajo esta norma.					

Fuente: OCI Auditoría MSPI 2025 Radicado No. 20251100092743 del 28/11/2025

8. ANÁLISIS DE BRECHA

La UAESP adopta el MSPI de acuerdo con la Política de Seguridad Digital y el Artículo 2. Ámbito de aplicación de la Resolución 500 de 2021, proferida por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC ¹ *“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.”*

De acuerdo con los lineamientos establecidos la OTIC realizó autoevaluaciones periódicas del nivel de implementación y madurez del (MSPI), adicionalmente la OCI en su rol evaluador realizó la auditoría al modelo utilizando la nueva perspectiva alineada con la ISO 27001:2022, la cual fue radicada con el No 20251100092743 del 28/11/2025. La cual se centró en el nivel de ejecución de los nuevos controles del modelo. Esta evaluación permitió identificar brechas de seguridad existentes y servirán como base para definir una hoja de ruta y las acciones necesarias para mejorar la postura de seguridad de la entidad.

FIGURA 2 AUTODIAGNÓSTICO MSPI 2025



Fuente: Propia tomada del Autodiagnóstico MSPI 2025

¹ [Documento maestro de los lineamientos del MSPI - MinTic.](#)

El autodiagnóstico realizado por la OTIC, arrojó una calificación promedio del 71%. Esto indica un nivel de madurez gestionado. Por lo tanto, el presente plan tiene como objetivo llevar a la Entidad a un nivel de madurez “Optimizado” mediante la implementación de los controles definidos en el MSPI de acuerdo con los recursos de la Entidad.

9. 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, las cuales están bajo la responsabilidad de la Oficina TIC:

TABLA 1 HOJA DE RUTA

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
(A.5) Controles Organizacionales	7	Inteligencia de amenazas	Definir, documentar y formalizar ante el SIG un procedimiento formal de inteligencia de amenazas, integrando fuentes externas	Elaborar y radicar en el SIG el procedimiento de inteligencia de amenazas	Procedimiento formal de inteligencia de amenazas de la seguridad	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			confiables y estableciendo análisis y documentando de manera periódica, que complementa la información del SIEM			
	23	Seguridad de la información para el uso de servicios en la nube	Definir, documentar, socializar y formalizar ante el SIG una política y procedimiento de gestión de servicios en la nube de acuerdo con los criterios establecidos con el	Elaborar y radicar en el SIG el procedimiento de gestión de nube	Procedimiento formal de gestión de nube	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			control			
	27	Aprendizaje sobre los incidentes de seguridad de la información	No se observa la cuantificación del impacto o costos de los incidentes de seguridad, tampoco se observa la mejora continua	Actualizar el procedimiento GTI-PC-16 Gestión de incidentes de seguridad de la información cumpliendo con lo solicitado en el control	Procedimiento GTI-PC-16 Gestión de incidentes de seguridad de la información actualizado	31/12/2026
	28	Recopilación de pruebas	No hay retención de logs, clasificación de registros, no se centralizan ni se almacenan	Definir y formalizar el procedimiento de gestión de logs	Procedimiento formal sobre gestión de logs	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			de forma segura. No se observa un proceso para destrucción controlada			
	29	Seguridad de la información durante la interrupción	No existen pruebas del plan de continuidad del negocio, no existe un análisis de procesos críticos y no se encuentran todos los procesos incluidos en el BCP	Diseñar y aprobar el plan de pruebas de continuidad del negocio en lo que corresponde a la OTIC Ejecutar las pruebas y documentar resultados	1. Plan de pruebas de continuidad del negocio en lo que corresponde a la OTIC 2- Informe de ejecución del plan de pruebas en lo que corresponde a la OTIC	30/04/2026 31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
				hallazgos y mejoras en lo que corresponde a la OTIC		
	30	Preparación de las TIC para la continuidad del negocio	Actualizar y formalizar los requisitos de continuidad TIC basados en los resultados del BIA y la evaluación de riesgos, definiendo RTO, RPO y capacidades de los sistemas, realizar y documentar las pruebas de DRP.	Actualizar el DRP-TI. Radicalo a la OAP solicitando evaluación/actualización del BCP	DRP-TI Actualizado. Documento que evidencie la solicitud a la OAP para que evalúen la pertinencia de actualizar el BCP de la entidad	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			Llevar a cabo la gestión necesaria para coordinar con OAP la actualización y pruebas del BCP lo que corresponde a la OTIC			
	34	Privacidad y protección de la Información de Identificación Personal (PII)	No se evidenció mecanismos que mitiguen el riesgo de fuga o divulgación no autorizada de información personal o sensible. (Data Loss Prevention,	Elaborar y formalizar el procedimiento PDP.	Procedimiento de Protección de Datos Personales (PDP)	30/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			o Prevención de Pérdida de Datos) Es decir, no se cuenta con una herramienta configurada y funcionando como mecanismo de protección de la información sensible de la entidad.			
	36	Cumplimiento de políticas, normas y estándares de seguridad de la información	Aunque se encuentran definidos los lineamientos para la revisión y protección de activos de	Convocar comité/ mesa técnica, revisar evidencias y levantar acta de verificación	Acta comité donde se verifica el cumplimiento de los procedimientos de las políticas y	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			información, no se observa documentación en las actas de comité primario u otra que permita evidenciar el cumplimiento o de control	n de estándares de seguridad	normas de seguridad	
(A.7) Controles Físicos	4	Supervisión de la seguridad física	Validar la posibilidad de que la OTIC cuente con sus propias cámaras y/o coordinar con la administración de RENOBO el acceso a los sistemas de monitoreo	Enviar solicitud formal a RENOBO/ Administración para acceso o autorización de cámaras	Solicitud formal para acceso a las cámaras del edificio o solicitud de autorización de las cámaras propiedad de la UAESP	30/06/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			del edificio		Si se recibe autorización, su instalación	
	7	Escritorio y pantalla despejados	Falta de factor de autenticación en algunas cuentas	Habilitar MFA en las cuentas definidas y generar informe de implementación	Informe de implementación del doble factor de autenticación en las cuentas que se determine sea necesario	31/12/2026
	13	Mantenimiento de equipos	Actualmente no hay plan de mantenimiento preventivo para equipos de cómputo.	Definir e implementar un plan de mantenimiento preventivo para la infraestructura	Plan de mantenimiento preventivo para la infraestructura tecnológica de la Entidad	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			Infraestructura onpremises obsoleta, algunos equipos repotenciados, pero sin soporte o sin contrato de mantenimiento especializado	tecnológica de la Entidad		
	14	Eliminación segura o reutilización de equipos	Se reutilizan equipos de cómputo sin asegurarse de realizar procesos de borrado seguro	Establecer lineamientos de borrado seguro y aplicarlos en bajas y reutilización	Procedimiento o lineamientos operativos para eliminación segura o borrado seguro en la reutilización de equipos	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
					de usuario final y servidores	
(A.8) Controles Tecnológicos	9	Gestión de la configuración	No se observa la aplicación de del manual de hardening y desarrollo seguro	Actualizar lineamientos y aplicar checklist de hardening ; emitir informe de aplicación	Manuales o lineamientos actualizados e informe de aplicación	31/12/2026
	11	Enmascaramiento de datos	No se observan procedimientos o controles técnicos para el enmascaramiento, seudonimiz	Evaluar casos de uso y emitir informe de aplicabilidad de enmascaramiento/a no minimizac	Informe de evaluación o revisión de en qué casos es aplicable el enmascar	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			ación o anonimización de información personal	ión	amiento de datos	
	12	Prevención de fuga de datos	No se evidenció mecanismos que mitiguen el riesgo de fuga o divulgación no autorizada de información personal o sensible. (Data Loss Prevention, o Prevención de Pérdida de Datos). Es decir, no se cuenta con una herramienta	Implementar políticas DLP, probar funcionamiento y documentar configuración	DLP implementado y documentado	31/07/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			configurada y funcionando como mecanismo de protección de la información sensible de la entidad			
	16	Actividades de seguimiento	Elaboración plan de pruebas de penetración (pentest). Realizar auditoría MSPI	Elaborar el plan de pruebas de penetración y presentarlo para aprobación Realizar autodiagnóstico MSPI	Plan Aprobado Autodiagnóstico MSPI actualizado	30/05/2026 31/12/2026
	22	Segregación de redes	No se evidencia segmentación	Levantar la segmentación	Diagramas de red evidencia	31/12/2026

DOMINIO	#	DESCRIPCIÓN	BRECHA	ACTIVIDAD	ENTREGABLE	FECHA
			ión clara y adecuada de la red	ción real y actualizar los diagramas de red con esa evidencia	ndo segmentación	

Nota: fuente elaboración propia basado en el autodiagnóstico del MSPI 2025

Como parte integral de la estrategia de seguridad digital, este documento 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 basada en el modelo; planificar, hacer, verificar y actuar (PHVA) de la seguridad y privacidad de la información, alineado con los objetivos estratégicos, normativos y el entorno digital de la entidad.

10. VERIFICACIÓN

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

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

De igual forma, el Oficial de seguridad de la información o quien haga sus veces en conjunto con la OTIC podrán realizar autoevaluaciones que consideren necesarias al MSPI, 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.

11. 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.

12. APROBACIÓN

TABLA 2 HOJA DE RUTA

Elaboró	Osbaldo Cortes Lozano – Profesional Universitario OTIC
Revisó	Jorge Alexis Rodriguez Meza – Jefe Oficina de Tecnologías de la Información y las Comunicaciones.
	Yuli Marcela Toro Pascagaza – Jefe Oficina Asesora de Planeación
Aprobó	Comité Institucional de Gestión y Desempeño – Acta de reunión xx/01/2026



ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UAESP

