PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UAESP

Enero 2024

ALCALDÍA MAYOR DE BOGOTÁ D.C.
UAESP
Unidad Administrativa Especial de Servicios Públicos
BOGOTÁ

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

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.

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

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).

1. 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.

2. OBJETIVO

Establecer una hoja de ruta integral que abarque las acciones esenciales para la implementación del habilitador de seguridad de la información de la Política Nacional de Gobierno Digital, soportado en el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y Comunicaciones MinTIC, preservando la confidencialidad, disponibilidad y privacidad de la información, así como la protección de los datos personales.

2.1 Objetivos Específicos

- Revisar el cumplimiento de los requisitos del MSPI mediante el instrumento dado por el MinTIC.
- Implementar acciones de mejora al Modelo de Seguridad y Privacidad de la Información.
- Aumentar el porcentaje de implementación de controles del Modelo de Seguridad y Privacidad de la Información en la Entidad que permitan llevar el nivel de madurez del modelo de “Gestionado” a “Optimizado”

3. 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”.
- Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.
- ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de 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.
- 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.
- 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.
- 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”.

4. 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.

5. ALCANCE

Aplica a todos los procesos de la UAESP, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información, el cual hace parte del Sistema Integrado de Gestión de la UAESP.

6. ANÁLISIS DE BRECHA

La Entidad hace uso de la herramienta diseñada por el MinTIC para autoevaluar la implementación y el nivel madurez del MSPI y las evaluaciones realizadas por la Oficina de Control Interno en noviembre de 2023 para tener una perspectiva más amplia en relación con el avance a la fecha y junto a la brecha encontrada definir la hoja de ruta y las acciones a desarrollar para la implementación del MSPI y alcanzar las metas definidas por el MinTIC a través del Decreto 1078 de 2015.

Figura 1 Autodiagnóstico MSPI noviembre 2024

Fuente: Propia

Como resultado de la última auditoria efectuada al Modelo de Seguridad y Privacidad de la Información, se obtuvo una calificación cuantitativa promedio de controles implementados del 83%.

El plan busca llevar a la Entidad un nivel de madurez del MSPI "**Optimizado**" implementando el 100% de los controles definidos en el MSPI.

7. 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	1	Actualizar las políticas	Políticas	Oficial de	01/07/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
seguridad de la información (A.1)		de seguridad y privacidad de la información.	actualizadas.	Seguridad de la Información.	
	2	Realizar autodiagnóstico MSPI.	Autodiagnóstico MSPI 2024	Oficial de Seguridad de la información	01/07/2024
Organización de la seguridad de la información (A.2)	3	Realizar inventarios de dispositivos móviles personales autorizados por la Entidad	Inventario de dispositivos móviles personales.	OTIC	31/07/2024
	4	Realizar divulgación de la resolución 648 del 2023 o aquella que la sustituya o haga sus veces.	Listado de asistencia	Oficial de Seguridad de la Información / OTIC	30/06/2024
Seguridad de los recursos Humanos (A.3)	5	Seguimiento a la implementación y firma de los acuerdos de confidencialidad por parte de funcionarios públicos.	Reportes del porcentaje de acuerdos firmados por personal de planta en la Entidad	Subdirección Administrativa y Financiera – Talento Humano	31/05/2024
Gestión de Activos (A.4)	6	Realizar la actualización del inventario de activos de información.	Inventario de activos de información aprobado por la	Todos los procesos	31/07/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
			Dirección.		
	7	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	30/04/2024
	8	Revisión de la pertinencia de actualizar el procedimiento de baja de bienes incluyendo la disposición final de activos críticos como equipos de cómputo cuando son donados o destruidos (borrado seguro para evitar que la información confidencial pueda ser copiada por personas no autorizadas).	Procedimiento actualizado o acta de reunión de pertenencia del procedimiento.	SAF - Apoyo Logístico	30/06/2024
	9	Revisión de la	Procedimiento	SAF – Talento	31/07/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
		pertinencia de actualizar el procedimiento retiro de servidores públicos teniendo en cuenta la devolución de activos físicos como equipos de cómputo, celulares, llaves físicas, tokens, entre otros.	actualizado o acta de reunión de pertenencia del procedimiento.	Humano	
Continuidad del Negocio (A.5)	10	Actualizar el plan de pruebas de continuidad del negocio.	BCP o Plan de pruebas actualizado.	OTIC	30/08/2024
Cumplimiento (A.6)	11	Revisar la implementación política y el Manual de Protección de Datos Personales.	Informe de análisis de brecha GAP – Datos Personales	Oficial de Datos Personales	01/07/2024
	12	Elaborar el plan de pruebas de penetración 2024.	Plan Aprobado	Oficial de Seguridad de la información / OTIC	30/04/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
	13	Identificación de repositorios de datos personales y las medidas técnicas implementadas para su protección.	Informe	Oficial de Datos Personales	01/07/2024
	14	Socializar lineamientos o recomendaciones para cumplir con el numeral 27.9 de la Resolución interna 757 del 2023 o aquella que lo sustituya o haga sus veces, en relación con el ítem AD 6.2.2 del MSPI.	Listado de asistencias	Oficial de Seguridad de la Información	01/07/2024
	15	Realizar auditoria al MSPI	Informe de Auditoria	OCI	31/12/2024
Control de Acceso (T.1)	16	Listar usuarios privilegiados	Informe o inventario	OTIC	01/05/2024
	17	Verificar el funcionamiento de las GPO y configuraciones necesarias en relación con la solicitud de cambio de contraseñas	Informe	OTIC	31/12/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
		la primera vez de uso y el cambio periódico de acuerdo con las políticas de seguridad definidas en la entidad.			
	18	Realizar campañas para cambios de contraseñas por parte de usuarios finales cuando han ocurrido incidentes de seguridad y privacidad de la información.	Campañas, piezas comunicativas o listados de asistencia.	Oficial de Seguridad de la Información.	30/08/2024
Criptografía (T.2)	19	Asegurar las conexiones entre aplicación y base de datos.	Informe aprobado por el jefe de la OTIC.	OTIC	31/04/2024
	20	Sensibilizar a servidores (as) públicos (as) y contratistas de la Entidad sobre la política de cifrado de la información y uso de controles criptográficos,	Listados de Asistencia y evaluación.	OTIC	30/04/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
		incluyendo la responsabilidad de los usuarios.			
	21	Verificar e implementar los mecanismos o configuraciones necesarias para el cifrado del correo electrónico.	Informe	OTIC	31/07/2024
Seguridad Física y del Entorno (T3)	22	Verificar condiciones de seguridad física y ambientales del cuarto eléctrico y la planta eléctrica.	Informe o acta de reunión.	Apoyo Logístico / OTIC	31/07/2024
	23	Revisar los derechos de acceso al cuarto eléctrico y la planta eléctrica.	Informe de registro de acceso.	OTIC	31/12/2024
Seguridad en las Operaciones (T.4)	24	Revisar el manejo de errores en sistemas de información y aplicativos	Informe.	OTIC	31/12/2024
	25	Revisar el registro de auditoría e información de logs de los sistemas de información y	Informe	OTIC	31/05/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
		aplicativos críticos			
	26	Actualizar el Capacity Planing	Capacity Planing actualizado	OTIC	31/07/2024
	27	Verificar y actualizar el procedimiento de gestión de respaldo de ser necesario.	Procedimiento actualizado o acta de reunión de pertenencia del procedimiento.	OTIC	30/03/2024
	28	Implementar los lineamientos para la gestión de respaldos de logs de acuerdo con las políticas de seguridad de la Entidad.	Informe de gestión de respaldos de logs	OTIC	31/12/2024
Seguridad en las comunicaciones (T.5)	29	Implementar doble factor de autenticación para dispositivos y aplicativos, siempre que ello lo permita.	Informe	OTIC	31/05/2024
	30	Actualizar el Capacity Planing	Capacity Planing actualizado	OTIC	31/12/2024
Seguridad	31	Realizar análisis de	Análisis de	OTIC	31/12/2024

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA
en los procesos de desarrollo y soporte		riesgos de seguridad de la información para los proyectos de software en fase de desarrollo o pruebas.	riesgos		
Gestión de incidentes de seguridad de la información (T.7)	32	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.	Oficial de seguridad de la información.	31/12/2024
	33	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	31/12/2024

Fuente: Elaboración Propia

Al integrar estas actividades, se busca fortalecer la resiliencia y la eficacia del MSPI, asegurando una gestión integral de la seguridad y privacidad de la información en el entorno digital.

8. VERIFICACIÓN

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

$$Cumplimiento\ del\ PSPI\ 2024 = \frac{Actividades\ Ejecutadas}{Actividades\ Planeadas} \times 100\%$$

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.

9. APROBACIÓN

Elaboró	Juan Sebastián Perdomo Méndez – Profesional Universitario OTIC
Revisó	Cesar mauricio Beltran Lopez – Jefe Oficina TIC Mesa Técnica de Seguridad Digital – Acta de reunión 18/01/2024
Aprobó	Comité Institucional de Gestión y Desempeño – Acta de reunión No 1 30/01/2024

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

UAESP

Unidad Administrativa Especial
de Servicios Públicos

BOGOTÁ