PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UAESP
Agosto 2022

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

Comité Institucional de Gestión y Desempeño

Director(a) General
Jefe(a) Oficina Asesora de Planeación
Jefe(a) Oficina Asesora de Comunicaciones
Jefe(a) Oficina de Tecnologías de Información y Comunicaciones
Subdirector(a) Administrativo y Financiero
Subdirector(a) Asuntos Legales.
Subdirector(a) Recolección Barrido y Limpieza.
Subdirector(a) Aprovechamiento
Subdirector(a) Disposición Final
Subdirector(a) Servicios Funerarios y Alumbrado público.

UAESP
Unidad Administrativa Especial
de Servicios Públicos

BOGOTÁ

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

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].

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

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

La implementación del plan de Seguridad y Privacidad de la Información en la Entidad está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

2. OBJETIVO

Establecer las actividades que permitan incrementar el nivel de madurez del MSPI implementado en la UAESP con base en el modelo PHVA (Planear-Hacer- Verificar-Actuar) definido en la norma NTC/IEC ISO 27001:2013, identificando en cada fase las actividades a realizar dentro de la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI), en el marco del modelo de referencia definido por el Ministerio de Tecnologías de la Información – MINTIC, el Modelo de Seguridad y Privacidad de la Información en concordancia con el Modelo Integrado de Planeación y Gestión -MIPG adoptado en la Entidad.

2.1 Objetivos Específicos

- Definir, actualizar, incluir o excluir los elementos normativos para proteger la información de la Entidad con base en los criterios de confidencialidad, integridad y disponibilidad.
- Gestionar los riesgos de Seguridad Digital de acuerdo con los lineamientos y políticas definidas por la Oficina Asesora de Planeación.
- Diseñar y ejecutar el plan de sensibilizaciones del Modelo de Seguridad y Privacidad de la Información para servidores(as) públicos(as), contratistas, con el objetivo de fortalecer conocimientos y capacidades frente a diferentes riesgos y amenazas de seguridad.
- Adelantar revisiones al MSPI con el fin de verificar el funcionamiento y cumplimiento normativo.
- Fortalecer los procedimientos relacionados al Modelo de Seguridad de la Información.
- Dar cumplimiento a la normatividad vigente en materia de Seguridad y Privacidad de la Información.

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 “.
- 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 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 la Resolución 313 de 2020 “Por medio de la cual se establecen las instancias de operacionalización del Sistema de Gestión y Sistema de Control Interno en la Unidad Administrativa Especial de Servicios Públicos, y se define otros lineamientos”.

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.

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 con apoyo del Oficial de Seguridad, 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.

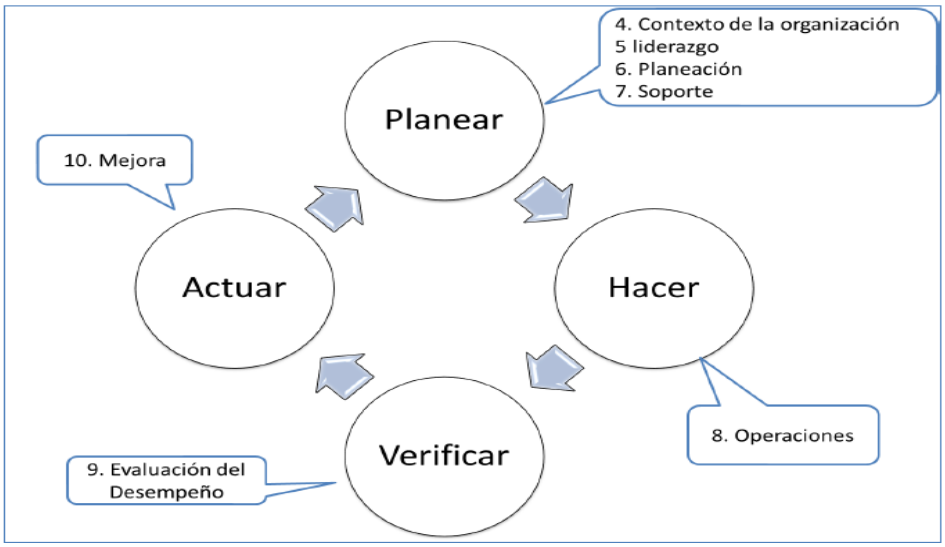
5. ALCANCE

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. EL MODELO PHVA

El Sistema de Gestión de la Seguridad de la Información (SGSI) inmerso dentro del MSPI, se basa en la necesidad que la Seguridad de la Información esté en continua evolución y que, además, dicha evolución esté documentada y justificada. El modelo en el que se basa el SGSI es denominado PHVA (Planear-Hacer-Verificar- Actuar). La Ilustración 1 representa la relación entre las fases del modelo y los numerales de la norma ISO 27001.

Ilustración 1 Modelo PHVA



Fuente NTC/IEC ISO 27001:2013

6.1 PLANEAR

En esta primera fase se realiza un estudio de la situación actual de la UAESP, desde el punto de vista de la seguridad y privacidad de la información, es necesario estimar las medidas que se van a implementar en función de las necesidades detectadas, determinando así el alcance del MSPI y la política de seguridad.

Se debe tener en cuenta que no toda la información de la UAESP tiene el mismo valor en cuanto a los tres pilares de seguridad (Confidencialidad, integridad y disponibilidad), e igualmente, no toda la información está sometida a los mismos riesgos. Por ello, una de las actividades principales dentro de esta fase es la realización de un Análisis de Riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos. Así mismo, se hace necesario el análisis de dichos riesgos con el fin de evaluar los posibles impactos para la Entidad y con base en ello, establecer planes de acción con miras a mitigar dichos riesgos.

6.1.1 Contexto de la Organización

En general, esta fase consiste en entender el contexto de la UAESP como Entidad que garantiza la prestación de los servicios públicos definidos dentro de su misionalidad, apoyándose en su visión, en su estructura jerárquica, en sus sistemas de información y en sus partes interesadas, e identificar los requisitos y expectativas de la seguridad de la información desde la perspectiva del cumplimiento de los requerimientos de usuario o parte interesada. Para ello es importante comprender los procesos y procedimientos en los que se soporta para cumplir sus objetivos, mirar el contexto interno y externo de la Entidad, definir los flujos de información con cada una de las partes interesadas y en general, comprender a la entidad como un Sistema, dando como resultado el entendimiento de la Entidad y a partir de eso, la definición del alcance del Sistema de Seguridad de Información, los objetivos del MSPI y la Política general de seguridad de la información en la Unidad Administrativa Especial de Servicios Públicos- UAESP.

El análisis de contexto organizacional se encuentra publicado en

https://www.uaesp.gov.co/transparencia/planeacion/planes pestaña Plan Estratégico Institucional.

6.1.2 Política de Seguridad de la Información

La UAESP ha adoptado la “Política General de Seguridad y Privacidad de la Información”, documento que contiene los principios y lineamientos generales para ser aplicados en el desarrollo de todas las actividades relacionadas con el tratamiento de la información de la Entidad, generando confianza en las partes interesadas. Así mismo, define los roles, obligaciones y responsabilidades en relación con la seguridad y privacidad de la información en la Entidad.

Así mismo, se adopta el Manual de Políticas de Seguridad y Privacidad de la Información que contiene los lineamientos orientados al cumplimiento de los controles de seguridad y privacidad de la información que permitan asegurar los tres pilares de seguridad de los activos de información de la Entidad y desarrollar de manera detallada la Política General de Seguridad y Privacidad de la Información

Las políticas mencionadas podrán ser consultadas en la página web de la Entidad en la sección de Transparencia y Acceso a la Información Pública.

6.1.3 Identificación y Clasificación de Activos de Información

Un activo de información, según la ley 1712 de 2014, es el elemento de información que la Unidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

La realización de un inventario y clasificación de activos hace parte de una administración de la seguridad y privacidad de la información efectiva dentro de una organización y contribuye al cumplimiento del control del Anexo A del estándar ISO/IEC 27001:2013 (inventario de activos, propiedad de activos, clasificación de la información, etiquetado y manipulado de la información). En la UAESP, las OTIC es el área encargada de consolidar y publicar la matriz de Activos de Información.

Las actividades que realiza la Oficina TIC para la gestión de Activos de Información se encuentran publicadas en el manual: GTI-MN-02 Clasificación de Activos de Información disponible en el micrositio del SIG-MIPG/Procesos de Apoyo/Gestión Tecnológica.

6.1.4 Análisis de Brecha

El análisis de brecha busca generar un diagnóstico relativo a la seguridad de la información basado en la identificación de diferencias entre el estado actual y el estado ideal de la Unidad Administrativa Especial de Servicios Públicos de acuerdo con los requerimientos exigidos en la norma NTC/IEC ISO 27001:2013, el Modelo de Seguridad y Privacidad de la Información - MSPI y las consideraciones definidas internamente como parte del ejercicio de la Entidad y el cumplimiento de su misionalidad.

Las fases para realizar una metodología de diagnóstico de seguridad de la información son:

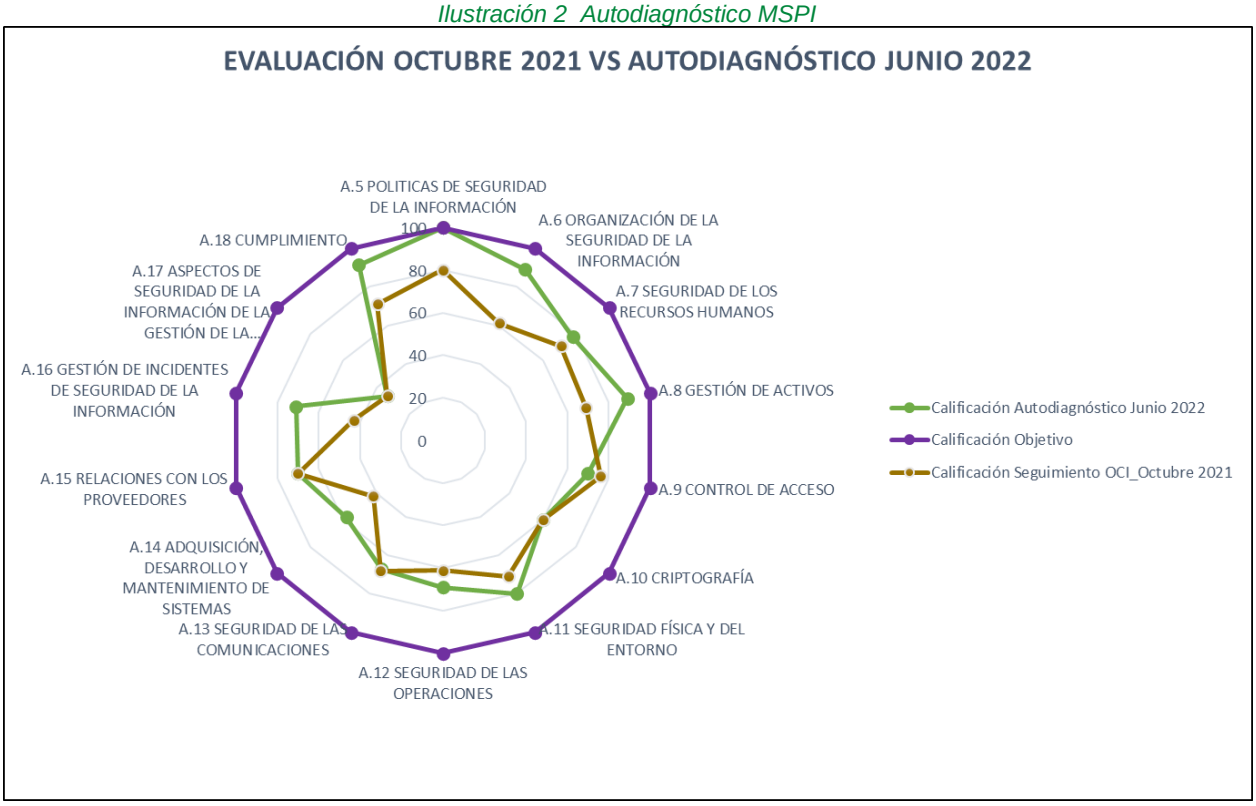
- Revisión del cumplimiento de las exigencias del Modelo de Seguridad y Privacidad de la Información - MSPI y la Norma NTC/IEC ISO 27001:2013 respecto a la Seguridad de la Información, la gestión de los riesgos, el análisis de vulnerabilidades y el seguimiento a las mismas.

- Revisión de los controles existentes que apliquen a la seguridad de la información en la UAESP según el anexo A de la citada Norma.

- Identificar requisitos desactualizados (Políticas, procedimientos, controles), los cuales son exigidos por la norma NTC/IEC ISO 27001:2013 y por el modelo del MinTic Modelo de Seguridad y Privacidad de la Información - MSPI.

La Oficina TIC hace uso de la herramienta diseñada por el MinTIC para autoevaluar la implementación y el nivel madurez del MSPI con corte a 30 de junio de 2022, de igual forma, se compara con la última evaluación realizada por la Oficina de Control Interno en octubre de 2021, 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

Ilustración 2 Autodiagnóstico MSPI



Fuente: Propia

Como resultado de la autoevaluación efectuada al Modelo de Seguridad y Privacidad de la Información, se obtuvo una calificación cuantitativa promedio de 73% frente al 63% del año 2021.

El plan busca llevar a la Entidad un nivel de madurez del MSPI "**Optimizado**" implementando el 100% de los controles definidos en el Modelo en el próximo año. De esta forma, la Entidad se propone para junio de 2023 acercarse al 100% de implementación de los controles definidos en el Modelo.

6.1.5 Metodología para la Gestión de Riesgos

La Oficina Asesora de Planeación, como líder de la Política de Administración de Riesgos, ha definido la metodología para la identificación y gestión riesgos en la Entidad en concordancia con los lineamientos del DAFP.

Este documento podrá ser consultado en la página web de la Entidad en la sección de Transparencia y Acceso a la Información Pública.

La Oficina TIC realizará seguimiento trimestral a los controles definidos en la matriz de riesgos de seguridad de la información como segunda línea de defensa con el acompañamiento de la Oficina Asesora de Planeación.

3

6.1.6 Plan de sensibilizaciones en Seguridad de la Información

El objetivo general es atender de manera oportuna las necesidades de sensibilizar en temas de seguridad de la Información a los servidores (as) públicos (as) y contratistas de la UAESP, permitiéndoles adquirir los conocimientos y habilidades necesarias para enfrentarse a los riesgos y amenazas de seguridad de la Información para apoyar el cumplimiento de las metas institucionales preservando la confidencialidad, integridad y disponibilidad de los activos de información.

El plan será definido e integrado al Plan Anual de Capacitaciones de la Entidad apoyado por el proceso de gestión de talento humano.

6.2 HACER

6.2.1 Operación

En esta fase se lleva a cabo el establecimiento de los controles de seguridad escogidos en la fase de planeación, junto con los seguimientos, actualizaciones y procesos de mejora propios. Dentro de esta fase se destaca el cumplimiento del plan de sensibilización en seguridad de la información, que conlleva a la concientización del personal de la UAESP de cara a que conozcan los controles implementados, el rolde todo(a)s lo(a)s servidoras y servidores, contratistas o partes interesadas desempeñan y sobre todo el buscar la colaboración de cada una de las personas como parte activa del sistema.

Dichos controles se especifican en la Matriz Identificación Riesgos Seguridad de la Información.

6.2.2 Métricas de Eficacia de los Controles y del Sistema.

Toda vez que el SGSI-MSPI es un sistema de mejora continua, es necesario definir parámetros precisos para evaluar el MSPI y en sí, la evolución del sistema en términos de justificar cada una de las acciones tomadas o en su defecto redirigir dichas acciones hacia la consecución de procesos más eficientes y efectivos. Por tal razón, se define un sistema de métricas e indicadores que permite obtener resultados de la ejecución del sistema, los cuales conllevan a medir la eficacia o eficiencia de los controles implementados, la consecución de objetivos y en general el nivel de implementación del sistema frente a la madurez de éste. Estos indicadores son:

- Nivel de madurez del MSPI
- Apropiación de conocimientos
- Tratamiento de eventos TI

6.2.3 Gestión del MSPI

La UAESP debe adoptar el Sistema de Gestión de Seguridad de la Información SGSI-MSPI, como parte integral y trasversal de la Entidad y como tal, debe gestionar las operaciones del Sistema mediante el seguimiento y revisión continua de todo el sistema, la evaluación y toma de decisiones frente a los resultados definidos por las métricas e indicadores adoptados y generando planes de mejoramiento para optimizar los resultados y corregir las falencias encontradas, todo esto confluyendo en auditorías internas y externas que demuestren la fortaleza o no del sistema desarrollado.

6.2.4 Gestión de Incidentes de Seguridad

La UAESP cuenta con el procedimiento y metodología para la Gestión de Incidentes de Seguridad de la información los cuales contemplan las etapas para el reporte, identificación y análisis de incidentes de seguridad de la información o eventos, que permitan gestionarlos de forma oportuna y adecuada mitigando el impacto a las posibles pérdidas de la confidencialidad, integridad y disponibilidad de la información o continuidad del negocio y operaciones de la Entidad. Los documentos mencionados se encuentran disponibles en el siguiente vínculo: GTI-IN-03 V1 Gestión de incidentes de seguridad de la información - GTI-PC-16 V1 Reporte de incidentes de seguridad de la información, disponible en el micrositio del SIG-MIPG/Procesos de Apoyo/Gestión Tecnológica

6.3 VERIFICAR

6.3.1 Evaluación de Desempeño

La UAESP dispone de mecanismos que le permiten evaluar la eficacia y éxito de los controles implementados. Por este motivo, toman especial importancia los registros (evidencias) que dejan los diferentes controles, así como los indicadores que permiten verificar el correcto funcionamiento del MSPI. En esta fase la UAESP:

1) Implementa procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos y determinar si las actividades de seguridad se desarrollan de acuerdo con lo previsto.
2) Revisa periódicamente la eficacia del MSPI mediante la evaluación y análisis de las métricas definidas para tal fin.

1) Indicadores de MSPI:
    a. Cumplimiento del Plan de Seguridad y Privacidad de la Información.
    b. Gestión de incidentes.
    c. Apropiación del conocimiento en temas de seguridad de la información.
2) Revisión periódica del estado de los activos de información, actualizando la matriz correspondiente y la matriz de riesgos, cuando corresponda.
3) Auditorías internas planificadas al Modelo.
4) Revisiones por parte de la alta dirección para asegurar el funcionamiento del MSPI para identificar oportunidades de mejora.
5) Actualiza los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión en el caso que sea necesario.
6) Mantiene registros de las actividades e incidentes que puedan afectar la eficacia del MSPI.

6.4 ACTUAR

6.4.1 Mejora Continua

En esta fase se llevarán a cabo las labores de mantenimiento y mejora del sistema de gestión de seguridad de información, seguimiento a riesgos, análisis de vulnerabilidades, hacking ético, así como las labores de mejora y de corrección si, tras la verificación, se ha detectado algún punto débil. Esta fase se puede llevar en paralelo con la verificación y se despliega al detectarse la deficiencia o hallazgo negativo, no esperando a adelantar una fase de verificación programada para comenzar con las tareas de mejora continua y corrección. En esta fase la UAESP:

1) Implementa y documenta las mejoras identificadas a través de los planes de mejoramiento interno y la gestión de cambios.
2) Toma medidas correctivas y preventivas y aplica las mejores prácticas sobre incidentes de seguridad por medio de las lecciones aprendidas que permitan actualizas los controles definidos en la Entidad.
3) Comunica las actividades y mejoras a todos los grupos de interés.
4) Actualización del Plan de Seguridad y Privacidad de la Información que permita alinear los objetivos propuestos del Modelo con los objetivos estratégicos de la Entidad y a los recursos disponibles.

7 PLAN DE ACCIÓN

De acuerdo con el análisis de la brecha encontrada del Modelo implementado en la Entidad, la Política General y el Manual de Seguridad y Privacidad de la Información, se definen las siguientes actividades para la implementación del MSPI.

Tabla 1 Plan de implementación MSPI

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
Política de seguridad de la información (A.1)	1	Revisar la conveniencia de la política general de seguridad y privacidad de la información.	Política actualizada. Nota: En caso de no requerir actualización por ser aun oportuna, socializar en mesa de seguridad digital y	Oficial de Seguridad de la Información.	01/02/2023	30/04/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
			entregar acta de reunión donde se evidencia la revisión y adecuación.			
	2	Realizar autodiagnóstico.	Autodiagnóstico e informe con recomendaciones presentado en la Mesa Técnica de seguridad Digital	Oficial de Seguridad de la información	01/02/2023	01/03/2023
Organización de la seguridad de la información (A.2)	3	Definir los lineamientos para la inclusión de la seguridad y privacidad de la información en la metodología de proyectos que tenga la Entidad.	Lineamientos documentados y aprobados	Oficina Asesora de Planeación	01/08/2022	22/02/2023
	4	Realizar, mínimo, dos divulgaciones de las Política de Seguridad y Privacidad de la Información, incluyendo roles y responsabilidades en seguridad de la información.	Asistencia y evaluación de la divulgación.	Oficial de Seguridad de la Información / OTIC	01/08/2022	28/03/2023
Seguridad de los recursos Humanos (A.3)	5	Definir los lineamientos de seguridad de la información como requisitos para los equipos usados en modalidad de teletrabajo.	Lineamientos o requerimientos documentados	OTIC	01/09/2022	09/12/2022
	6	Definir acuerdos de confidencialidad en relación con las responsabilidades de los contratistas, servidores (as) públicos (as) y la UAESP con la seguridad y privacidad de la información. Nota: Se deberá incluir los tiempos de cobertura (Antes, Durante y Después), responsabilidades, uso permitido de la información, notificación en caso de incidentes o fugas de información y acciones en caso de incumplimiento.	Acuerdos, clausulas, o el mecanismo adecuado. Nota: Si no es requerido por algún motivo, deberá entregarse el concepto legal.	Subdirección de Asuntos Legales - Contratación	01/06/2022	31/12/2022
	7		1. Formato de Acuerdo de confidencialidad incorporado al Procedimiento de vinculación de personal. 2, Acuerdos de confidencialidad del personal de planta activo diligenciados, firmados e incorporados en los expedientes laborales.	Subdirección Administrativa y Financiera - Talento Humano	1/09/2022	31/12/2022
	8	Formular o actualizar el plan de Sensibilizaciones y Capacitaciones de Seguridad y Privacidad de la información 2022 y 2023.	Plan aprobado	Oficial de Seguridad de la Información	01/08/2022	01/02/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
		Nota: Este plan debe estar alineado con el Plan Anual de Capacitaciones..				
	9	Hacer seguimiento al Plan de Capacitaciones y Comunicaciones de Seguridad y Privacidad de la información Vigencias 2022 y 2023	Informe de Seguimiento y evidencias de la ejecución del Plan	Oficial de Seguridad de la Información	1/08/2023	30/04/2023
	10	Socialización de los procedimientos de Gestión Disciplinaria Interna, reporte, investigación y posibles sanciones.	Listado de Asistencia y evaluación de la divulgación.	Control Interno Disciplinario	01/09/2022	31/12/2022
Gestión de Activos de información (A.4)	11	Revisar o actualizar, de ser necesario, los lineamientos para el inventario de activos de información.	Procedimiento o lineamientos actualizados. Nota: Si no se requiere actualización, acta de reunión de la revisión.	OTIC / Gestión Documental .	01/11/2022	15/12/2022
	12	Definir los lineamientos para el etiquetado de información.	Procedimiento o lineamientos actualizados.	OTIC/ Gestión Documental / Planeación	01/11/2022	15/12/2022
	13	Implementar los lineamientos para el etiquetado de información.	Muestra de información física y Digital etiquetada	OTIC/ Gestión Documental / Planeación	16/12/22	31/03/2023
	14	Realizar la actualización del inventario de activos de información.	Inventario de activos de información aprobado por la Dirección	OTIC	1/11/22	15/12/2022
	15	Socializar al personal de la Entidad el procedimiento para la devolución de activos de información una vez finalice la vinculación con la Entidad o cualquier situación administrativa que lo amerite.	Asistencia y evaluación de la divulgación.	Subdirección Administrativa y Financiera - Talento Humano	1/09/2022	31/10/2022
	16	Revisar la aplicación de controles de seguridad para medios removibles.	Informe de controles aplicados sobre dispositivos de almacenamiento removible.	Oficial de Seguridad de la Información.	01/10/2022	30/04/2023
Continuidad del Negocio (A.5)	17	Elaborar el Plan de Continuidad del negocio que incluya las estrategias de recuperación, procedimientos adecuados ante incidentes o eventos no deseados, vuelta a la normalidad y requisitos	Plan aprobado por el CIGD	Oficina Asesora de Planeación	1/08/2022	31/03/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
		de seguridad de la información.				
	18	Elaborar y ejecutar el plan de pruebas de continuidad del negocio.	Informe y recomendaciones para la mejora o actualización del Plan de continuidad del negocio, de acuerdo con el resultado del plan de pruebas, presentado al CIGD. Nota: El informe deberá contener los resultados del plan de pruebas del DRP y otros que apliquen.	Oficina Asesora de Planeación O. Tic´s y Equipo de Salud y seguridad en el trabajo de la SAF.	1/08/2022	31/03/2023
	19		Informe del plan de pruebas del DRP ejecutado y recomendaciones, cuando apliquen. Nota: El informe deberá estar consolidado en el informe del plan de continuidad del negocio.	OTIC.	31/10/2022	30/04/2023
Cumplimiento (A.6)	20	Sensibilizar a contratistas y servidores (as) públicos (as) sobre derechos de autor	Listado de Asistencia y evaluación de la divulgación.	Oficial de Datos Personales / SAL.	1/06/2022	31/03/2023
	21	Documentar el ciclo de vida para la seguridad y protección de Datos Personales.	Documento aprobado.	Oficial de Datos Personales	01/08/2022	09/12/2022
	22	Auditoría interna MSPI.	Informe de Auditoria	Oficina de Control Interno	1/10/2022	31/12/2022
	23	Pruebas de penetración a los sistemas de información críticos de la Entidad.	Informe de ejecución de pruebas de penetración o PENTEST.	OTIC	01/12/2022	31/12/2022
	24	Definir acuerdos de confidencialidad con para proveedores y ANS que mitiguen riesgos de fuga de información y los asociados a la cadena de suministro.	Acuerdos, clausulas o el mecanismo adecuado, implementado.	SAL - Contratación	1/06/2022	31/12/2022
	25	Realizar periódicamente la revisión de derechos de acceso a los sistemas de información de la Entidad de acuerdo con el procedimiento de gestión de usuarios, incluyendo los usuarios privilegiados o administradores.	Informe o comunicaciones oficiales.	OTIC en conjunto con todos los Procesos.	01/08/2022	31/12/2022

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
Control de Acceso (T.1)	26	Realizar prueba concepto para implementación de un sistema de autogestión de contraseñas integrando el Directorio Activo.	Informe presentado al jefe de la OTIC	OTIC	01/08/2022	31/10/2022
	27	Implementar mecanismo de autogestión de contraseñas.	Mecanismo implementado	OTIC	01/01/2023	30/04/2023
	28	Exigir el uso de contraseñas robustas de acuerdo con los lineamientos definidos por la OTIC y las políticas de seguridad de la información.	Informe de configuración e implementación de contraseñas robustas para los sistemas de información y recursos tecnológicos de la Entidad.	OTIC	15/08/2022	30/10/2022
	29	Controlar los derechos de acceso de usuarios privilegiados.	Matriz de usuarios con acceso privilegiados y autorizados por la OTIC.	OTIC	15/08/2022	30/10/2022
Criptografía (T.2)	30	Pruebas para el aseguramiento de conexiones entre aplicación y base de datos.	Informe presentado al jefe de la OTIC.	OTIC	01/08/2022	30/11/2022
	31	Implementación del aseguramiento entre aplicaciones y bases de datos.	Informe presentado al jefe de la OTIC.	OTIC	01/10/2022	30/11/2022
	32	Implementar mecanismos para la gestión de llaves	Informe presentado al jefe de la OTIC.	OTIC	01/08/2022	30/11/2022
	33	Revisión matriz de riesgos de seguridad digital.	Informe a todos los procesos con las recomendaciones sobre los controles implementados.	Oficial de Seguridad de la Información / Planeación	01/11/2022	31/01/2023
	34	Definir lineamientos para el uso de firmas mecanografiadas, digitales o electrónicas en la Entidad.	Lineamiento, directriz o documento equivalente.	Gestión Documental	1/08/2022	30/10/2022
Seguridad Física y del Entorno (T3)	35	Definir controles de seguridad física para las áreas seguras de la Entidad.	Listado de las áreas seguras y verificación de controles de acceso implementados de acuerdo con el ítem T3.1.1 y T3.1.5 del autodiagnóstico del MSPI	Apoyo Logístico	1/08/2022	31/12/2022
	36	Revisión de riesgos ambientales y amenazas externas	Riesgos y Mecanismos controles de mitigación documentados	Oficina Asesora de Planeación / SAF - Apoyo Logístico Equipo de Salud y seguridad en el trabajo de la SAF	1/08/2022	31/03/2023
	37	Revisión del estado y	Informe y corrección de	OTIC	15/12/2022	01/03/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
		funcionamiento del centro de cableado eléctrico y de datos de las sedes de la Entidad.	las anomalías o desviaciones de normas eléctricas (RETIE) y de red de datos.			
	38	Definir los lineamientos para el retiro de activos de información de la Entidad.	Lineamientos documentados y aprobados por la SAF / Dirección.	SAF -Apoyo logístico	1/08/2022	31/12/2022
	39	Definir puntos de control para la disposición segura de medios de almacenamiento de la Entidad.	Lineamientos o documentos aprobados.	SAF -Apoyo logístico	1/08/2022	31/12/2022
Seguridad en las Operaciones (T.4)	40	Documentar el control para instalación de software y aplicativos en la Entidad.	Documento aprobado.	OTIC	01/08/2022	30/10/2022
	41	Informe de gestión de capacidad o Capacity Planning que incluya aspectos como: Necesidad de expansión, desempeño, capacidad del ancho de banda y futuras necesidades cuando las hubiera.	Informes periódicos presentados al jefe de la OTIC semestralmente.	OTIC	01/08/2022	30/04/2023
	42	Probar el proceso de restauración de respaldos de forma periódica.	Cronograma e informes y recomendaciones de las pruebas ejecutadas.	OTIC	01/08/2022	30/04/2023
	43	Ajustar el correlacionador de eventos, incluyendo los logs de los diferentes sistemas de seguridad.	Reportes o informes mensuales con el análisis del correlacionador de eventos y la definición del almacenamiento de los logs que mitigue los errores por sobrepasar su capacidad u otra limitante. Nota: De no ser posible lo anterior, se debe documentar el análisis analizar de los reportes de las diferentes herramientas de seguridad.	OTIC	01/08/2022	30/04/2023
	44	Documentar las buenas practicasprácticas establecidas en la política de desarrollo de software y el Manual definido por la OTIC.	Documentación para los sistemas de información en desarrollo: • Solicitudes de cambio y análisis de riesgos. • Cronograma • Casos de uso • Requisitos Funcionales / No funcionales • Plan de pruebas	OTIC	01/08/2022	30/04/2023

DOMINIO	#	ACTIVIDADES	ENTREGABLE	RESPONSABLE	FECHA INICIO	FECHA FIN
			funcionales y de seguridad. Criterios de aceptación.			
Seguridad en las comunicaciones (T.5)	45	Pruebas para implementación de mecanismos de controles de acceso a la red.	Informe de los mecanismos probados y recomendaciones.	OTIC	01/08/2022	31/10/2022
	46	Implementación de mecanismos de control de acceso a la red.	Informe del mecanismo implementado, donde se evidencia las respectivas pruebas.	OTIC	01/11/2022	28/02/2023
	47	Definir lineamientos de seguridad para conexión a la red.	Procedimiento de comunicación.	Oficial de seguridad de la información /OTIC	01/08/2022	31/12/2022
	48	Implementar el procedimiento o proceso para el acceso a datos de pruebas.	Documentación que evidencie las autorizaciones y el tipo de datos al que se va a tener acceso.	OTIC	01/08/2022	30/10/2022
Gestión de incidentes de seguridad de la información (T.7)	49	Definir protocolo de atención y respuesta a incidentes de seguridad de la información por tipo de incidente.	Protocolo o procedimiento documentado, incluyendo responsabilidades.	Responsable de seguridad de la información / OTIC	01/08/2022	31/10/2022
	50	Documentar informes de incidentes de seguridad de la información clasificados como altos o muy altos.	Informes de incidentes que incluya la investigación, recolección de evidencia, lecciones aprendidas, contactos con autoridades, recomendaciones para actualizar la gestión de incidente, cuando corresponda, entre otros.	Responsable de seguridad de la información	01/08/2022	30/04/2023

Fuente Propia

Es importante que a los controles establecidos sobre el 100% en el autodiagnóstico, se les debe realizar monitoreo a través de la instancia que se considere oportuna y que permita el mantenimiento y mejora continua del Modelo.