Un dibujo con letras

Descripción generada automáticamente con confianza media

**PLAN DE**

**SEGURIDAD Y**

**PRIVACIDAD**

**DE LA INFORMACIÓN**

***UAESP***

***Enero 2022***

***Imagen que contiene Gráfico

Descripción generada automáticamenteComité 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.

Imagen que contiene texto, tarjeta de presentación, dibujo

Descripción generada automáticamente

TABLA DE CONTENIDO

[ÍNDICE DE ILUSTRACIONES 5](#_Toc93585125)

[TÉRMINOS Y DEFINICIONES 6](#_Toc93585126)

[1. INTRODUCCIÓN 7](#_Toc93585127)

[2. OBJETIVO 8](#_Toc93585128)

[2.1 Objetivos Específicos 8](#_Toc93585129)

[3. REFERENCIA NORMATIVA 8](#_Toc93585130)

[4. RESPONSABLES DE LA IMPLEMENTACIÓN 9](#_Toc93585131)

[5. ALCANCE PLAN MSPI 9](#_Toc93585132)

[6. EL MODELO PHVA 9](#_Toc93585133)

[6.1 PLANEAR 10](#_Toc93585134)

[6.1.1 Contexto de la Organización 10](#_Toc93585135)

[6.1.2 Política de Seguridad de la Información 11](#_Toc93585136)

[6.1.3 Identificación y Clasificación de Activos de Información 11](#_Toc93585137)

[6.1.4 Análisis de Brecha 11](#_Toc93585138)

[6.1.5 Metodología para la Gestión de Riesgos 13](#_Toc93585139)

[6.1.6 Plan de sensibilizaciones en Seguridad de la Información 13](#_Toc93585140)

[6.2 HACER 13](#_Toc93585141)

[6.2.1 Operación 13](#_Toc93585142)

[6.2.2 Métricas de Eficacia de los Controles y del Sistema. 13](#_Toc93585144)

[6.2.3 Gestión del MSPI 14](#_Toc93585145)

[6.2.4 Gestión de Incidentes de Seguridad 14](#_Toc93585146)

[6.3 VERIFICAR 14](#_Toc93585147)

[6.3.1 Evaluación de Desempeño 14](#_Toc93585148)

[6.4 ACTUAR 15](#_Toc93585149)

[6.4.1 Mejora Continua 15](#_Toc93585150)

[7 PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 15](#_Toc93585151)

**ÍNDICE DE TABLAS**

[**Tabla 1 Plan de implementación MSPI 15**](#_Toc93579652)

# 

# ÍNDICE DE ILUSTRACIONES

[**Ilustración 1 Modelo PHVA 10**](#_Toc93585209)

[**Ilustración 2 Autodiagnóstico MSPI 12**](#_Toc93585210)

# 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).

# 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.

# OBJETIVO

Describir 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.

# 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.

# 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 tal motivo, la Oficina TIC como líder de la Política de Seguridad Digital, por medio de la mesa técnica se enfocará en hacer seguimiento a la Implementación del Modelo de Seguridad y Privacidad de Información – MSPI en la Entidad.

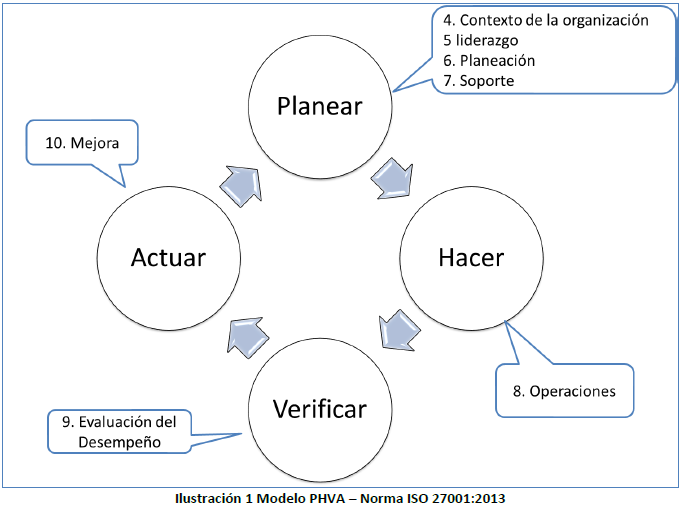
# ALCANCE PLAN MSPI

Aplica a 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.

# 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.

# 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.

# Política de Seguridad de la Información

La Alta Dirección apoyada en el Comité Institucional de Gestión y Desempeño buscará establecer controles administrativos y operativos, que regulen de manera efectiva el acceso de los usuarios de los sistemas a nivel de aplicación, sistema operativo, bases de datos, red y acceso físico.

Teniendo en cuenta lo anterior, se adopta el Manual de las políticas de Seguridad de la Información de cumplimiento por parte de servidores(as) públicos(as), contratistas y terceros que accedan a la información de la Entidad, usen equipos informáticos y de comunicaciones, interactúen con herramientas tecnológicas o servicios informáticos e ingresen de manera física o lógica a las instalaciones de la Unidad.

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.

La Política General de Seguridad y Privacidad de la información se encuentra publicada en <https://www.uaesp.gov.co/content/politica-seguridad-la-informacion>

# 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.

# 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.

En cumplimiento con lo establecido por el MINTIC, se usa la herramienta de autodiagnóstico de seguridad y privacidad de la información la cual arroja un resultado que permite a cada entidad visualizar los diferentes dominios de la norma, evaluar las falencias y a partir de esto, generar un plan de seguridad de la información para ser desarrollado al interior de esta y dar cumplimiento con lo estipulado en el manual de gobierno digital en sus diferentes componentes. En este sentido, al aplicar la herramienta, con corte a octubre de 2021, se generaron los siguientes resultados:

Ilustración 2 Autodiagnóstico MSPI

Interfaz de usuario gráfica

Descripción generada automáticamente

Fuente: Propia

Como resultado de la evaluación efectuada al Modelo de Seguridad y Privacidad de la Información, se tuvo una calificación cuantitativa promedio de 63% frente al 53% del año 2020.

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 los próximos dos años. De esta forma, la Entidad se propone para el 2022 acercarse a un promedio de 85% de implementación de los controles del MSPI y durante el segundo año (2023) llegar y mantener al 100% la implementación de estos y su nivel de madurez.

# Metodología para la Gestión de Riesgos

La Oficina Asesora de Planeación es la encargada de liderar la Política de Administración de Riesgos en la Entidad donde los procesos identificara los diferentes riesgos establecidos (Gestión, corrupción y de seguridad de la Información), este documento puede ser consultado en el sistema integrado de gestión en la página web institucional.

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

# 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(as) servidoras y servidores públicos 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.

# HACER

# 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, proceso que lo lidera la OAP.

# 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

# 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.

# 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](https://www.uaesp.gov.co/sig/documentos/gestionti/editables/GTI-IN-03%20V1%20Gestion%20de%20incidentes%20de%20seguridad%20de%20la%20informacion.pdf) - [GTI-PC-16 V1 Reporte de incidentes de seguridad de la información](https://www.uaesp.gov.co/sig/documentos/gestionti/editables/GTI-PC-16%20V1%20Reporte%20de%20incidentes%20de%20seguridad%20de%20la%20informacion.pdf), disponible en el micrositio del SIG-MIPG/Procesos de Apoyo/Gestión Tecnológica

# VERIFICAR

# 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.
3. Revisa periódicamente el estado de los activos de información, actualizando periódicamente la matriz correspondiente y la matriz de riesgos
4. Revisa periódicamente la evaluación de riesgos, actualizando el Plan de tratamiento de riesgos.
5. Realiza Auditorías internas planificadas.
6. Adelanta revisiones por parte de la alta dirección para asegurar el funcionamiento del MSPI para identificar oportunidades de mejora.
7. Actualiza los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión en el caso que sea necesario.
8. Mantiene registros de las actividades e incidentes que puedan afectar la eficacia del MSPI.

# ACTUAR

# 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.
  2. Toma medidas correctivas y preventivas y aplica las mejores prácticas sobre incidentes de seguridad, provenientes de experiencias de seguridad propias y de terceros documentadas.
  3. Comunica las actividades y mejoras a todos los grupos de interés.
  4. Busca que las mejoras realizadas al MSPI cumplan los objetivos previstos y que estén enfocadas a las necesidades y requerimientos de la Entidad.

# PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Seguridad y Privacidad de la Información comprende el siguiente cronograma y para su cumplimiento en las fechas establecidas se realizará su respectivo seguimiento:

Tabla 1 Plan de implementación MSPI

|  |  |  |  |
| --- | --- | --- | --- |
| GESTIÓN | ACTIVIDADES | RESPONSABLE DE LA TAREA | FECHAS PROGRAMACIÓN TAREAS |
| **Documentación**  **MSPI.** | Actualizar el documento Manual de Políticas de Seguridad y Privacidad de la Información. | Oficina TIC. | 1/06/2022. |
| Actualizar el Plan Auditoria Pentest. | Oficina TIC. | 28/03/2022. |
| Actualizar y aprobar el Plan de Sensibilizaciones del MSPI. | Oficina TIC. | 30/01/2022. |
| Actualizar la Declaración de aplicabilidad (SOA). | Oficina TIC. | 31/08/2022. |
| Actualizar los Procedimientos, Instructivos, Manuales con relación al MSPI. | Oficina TIC. | 31/12/2022. |
| Revisar los lineamientos para el levantamiento de activos de información. | Oficina TIC. | 30/01/2022. |
| **Relación con proveedores/ transferencias de información.** | Definir los Acuerdos de confidencialidad con proveedores y terceros. | Oficina TIC/ Subdirección de Asuntos Legales. | 30/06/2022. |
| **Gestión de riesgos Riesgos de Seguridad de la Información.** | Identificar y gestionar Riesgos de Seguridad de la Información. | Oficina TIC. | 31/12/2022. |
| Realizar el Seguimiento a la Matriz de Riesgos de Seguridad de la Información. | Oficina TIC. | 31/12/2022. |
| **Gestión de Incidentes de Seguridad de la Información.** | Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información  Gestionar los incidentes de Seguridad de la Información identificados. | Oficina TIC. | 31/12/2022. |
| **Gestionar los incidentes de Seguridad de la Información identificados.** | Diligenciar la bitácora de incidentes de seguridad y privacidad la información. | Oficina TIC. | 31/12/2022. |
| Reportar ante el CSIRT algún tipo de materialización de Incidentes de Seguridad de la Información. | Oficina TIC. | 31/12/2022. |
| Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI. | Oficina TIC. | 31/12/2022. |
| **Plan de recuperación de desastres- DRP** | Elaborar la Documentación relacionada al DRP. | Oficina TIC. | 01/08/ 2022 |
| **Continuidad del Negocio- BCP** | Elaborar el plan Continuidad del negocio de la Entidad. | Oficina Asesora de Planeación/ Subdirección Administrativa y Financiera/ Oficina TIC. | 31-12-2022 |
| **Implementación del Plan Continuidad Servicios de TI** | Aprobar y adoptar del Plan de continuidad de servicios de TI. | Oficina TIC. | 31/12/2022 |
| **Seguridad de las Operaciones** | Apoyar en las Auditorías Internas y Externas al MSPI. | Oficina TIC. | 31/12/2022 |
| Actualizar y ejecutar auditoria el Plan de pruebas de penetración en entornos controlados- Pentest. | Oficina TIC. | 28/03/2022 |
| Elaborar del plan y ejecución de las pruebas a la Continuidad de los servicios críticos de TI. | Oficina TIC. | 28/03/2022 |
| **Revisión de los controles de la norma ISO 27001:2013** | Revisar periódicamente de los controles de la norma ISO 27001:2013. | Oficina TIC. | 1/06/2022 |
| **Indicadores MSPI** | Formular, Implementar, actualizar y reportar los indicadores del MSPI. | Oficina TIC. | 31/12/2022 |
| **Protección de datos personales** | Actualizar la Política para el tratamiento de Datos Personales. | Oficina TIC. | 1/07/2022 |
| Actualizar el documento Manual de Políticas de Seguridad de la Información donde se establezcan los lineamientos para cuando el equipo de desarrollo acceda a Datos Sensibles. | Oficina TIC. | 1/07/2022 |
| Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC. | Oficina TIC. | 31/03/2022. |
| Revisar las bases de datos personales recolectadas. | Oficina TIC. | 1/07/2022. |
| Registrar y actualizar las bases de datos personales ante la Superintendencia de Industria y Comercio- SIC. | Oficina TIC. | 1/07/2022. |

Fuente Propia