

**PLAN DE SEGURIDAD**

**Y PRIVACIDAD DE LA**

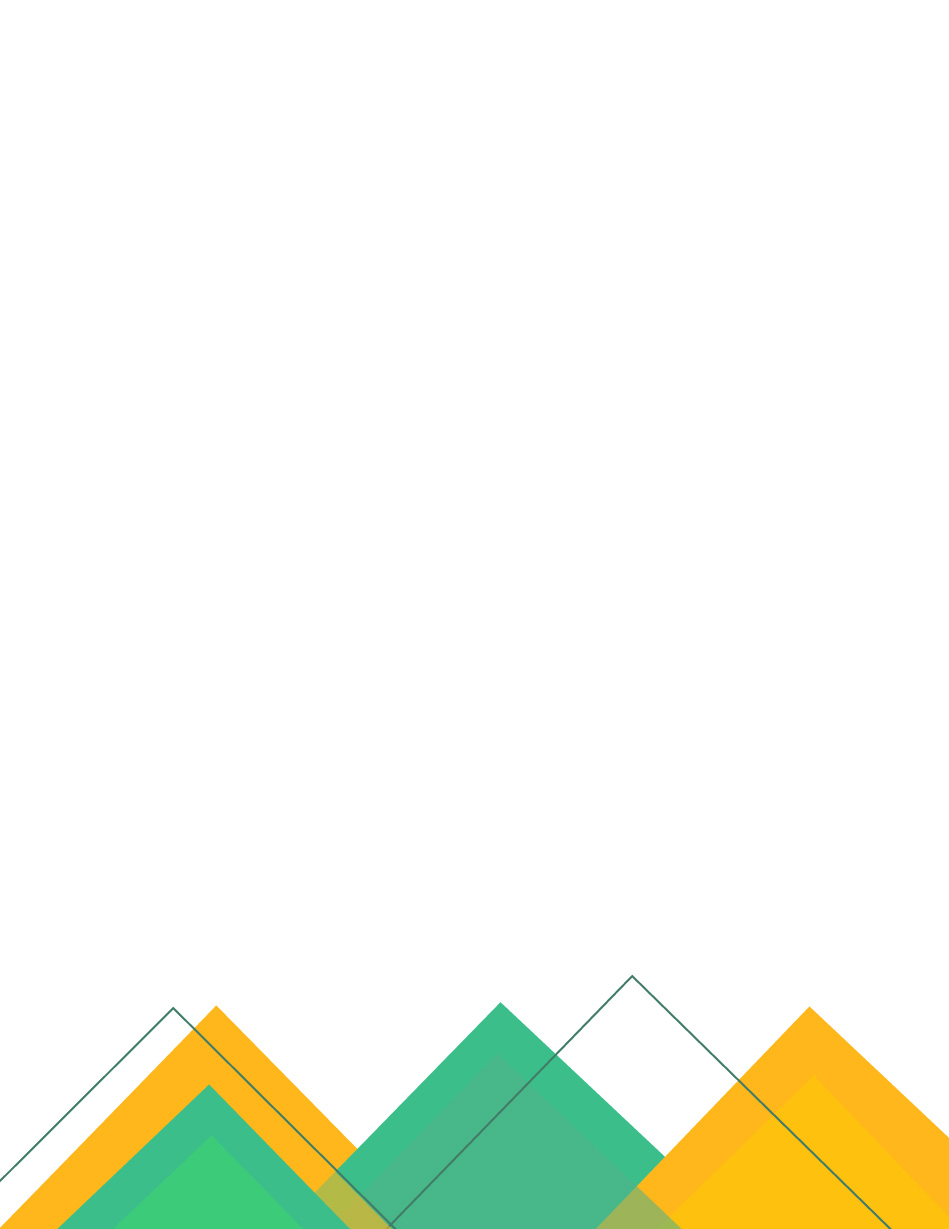
**INFORMACIÓN**

***OFICINA DE TECNOLOGIAS DE***

***LA INFORMACIÓN Y LAS***

***COMUNICACIONES***

***Enero 2021***



***Luz Amanda Camacho***

***Directora General***

***César Mauricio Beltrán López***

***Jefe Oficina de Tecnologías de la Información y las Comunicaciones***

***Comité Institucional de Gestión y Desempeño***

*Julián Camilo Amado Velandia*

*Andrés Pabón Salamanca*

*Ingrid Lisbeth Ramírez Moreno*

*Álvaro Raúl Parra Eraso*

*Hermes Humberto Forero Moreno*

*Fredy Ferley Aldana Arias*

*Rubén Darío Perilla Cárdenas*

*Carlos Arturo Quintana Astro*

***Equipo de trabajo***

*Sayra Paola Nova Murcia*

*Juan Sebastián Perdomo Méndez*

*Osbaldo Cortes Lozano*

*Gisela Arias Salazar*

*Rubén Esteban Buitrago Daza*





TABLA DE CONTENIDO

[ÍNDICE DE TABLAS 6](#_Toc61020454)

[ÍNDICE DE ILUSTRACIONES 7](#_Toc61020455)

[GLOSARIO 8](#_Toc61020456)

[1. INTRODUCCIÓN 9](#_Toc61020457)

[2. OBJETIVO DEL DOCUMENTO 9](#_Toc61020458)

[3. DOCUMENTO DE REFERENCIA 9](#_Toc61020459)

[4. RESPONSABLES DE LA IMPLEMENTACIÓN 9](#_Toc61020460)

[5. ALCANCE PLAN MSPI 10](#_Toc61020461)

[6. OBJETIVO PLAN MSPI 10](#_Toc61020462)

[6.1 Objetivos Específicos Plan MSPI 10](#_Toc61020463)

[7. EL MODELO PHVA 11](#_Toc61020464)

[7.1 PLANEAR 11](#_Toc61020465)

[7.1.1 Contexto de la Organización 12](#_Toc61020466)

[7.1.2 Políticas de Seguridad de la Información 12](#_Toc61020467)

[7.1.3 Identificación y Clasificación de Activos de Información 13](#_Toc61020468)

[7.1.4 Análisis de Brecha 14](#_Toc61020469)

[7.1.5 Documentación de Procedimientos 16](#_Toc61020470)

[7.1.6 Metodología para la Gestión de Riesgos 16](#_Toc61020471)

[7.1.7 Programas de Sensibilización y/o Formación de Empleados 17](#_Toc61020472)

[7.1.8 Gestión de los Recursos del SGSI-MSPI 18](#_Toc61020473)

[7.1.9 Soporte 18](#_Toc61020474)

[7.1.9.1 Recursos 18](#_Toc61020475)

[7.1.9.2 Competencia 18](#_Toc61020476)

[7.1.9.3 Toma de Conciencia 19](#_Toc61020477)

[7.1.9.4 Comunicación 19](#_Toc61020478)

[7.1.9.5 Información Documentada 19](#_Toc61020479)

[7.2 HACER 20](#_Toc61020480)

[7.2.1 Operación 20](#_Toc61020481)

[7.2.2 Métricas de Eficacia de los Controles y del Sistema. 20](#_Toc61020488)

[7.2.3 Gestión de Funcionamiento normal del MSPI 20](#_Toc61020489)

[7.2.4 Gestión de Incidentes de Seguridad 20](#_Toc61020490)

[7.3 VERIFICAR 21](#_Toc61020491)

[7.3.1 Evaluación de Desempeño 21](#_Toc61020492)

[7.4 ACTUAR 21](#_Toc61020493)

[7.4.1 Mejora Continua 21](#_Toc61020494)

[8 PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 22](#_Toc61020495)

# ÍNDICE DE TABLAS

[Tabla 1: Competencias 18](#_Toc61015540)

[Tabla 2: Plan de implementación 26](#_Toc61015541)

# 

# 

# ÍNDICE DE ILUSTRACIONES

[Ilustración 1 Modelo PHVA 11](#_Toc61016436)

[Ilustración 2 Autodiagnóstico MSPI 15](#_Toc61016437)

[Ilustración 3. Administración del riesgo en seguridad de la información 17](#_Toc61016438)

# GLOSARIO

Activo: cualquier cosa que tenga valor para la organización.

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.

Confidencialidad: la propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados

Integridad: la propiedad de salvaguardar la exactitud e integridad de los activos.

**Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

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.

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.

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 las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

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

# 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, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

# OBJETIVO DEL DOCUMENTO

Este documento busca describir las actividades del plan de seguridad y privacidad de la información con base en el modelo PHVA (Planear-Hacer- Verificar-Actuar) definido en la norma ISO 27001, 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-MSPI y en concordancia con el Modelo Integrado de Planeación y Gestión -MIPG adoptado en la Entidad.

# DOCUMENTO DE REFERENCIA

* 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.

# 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 mesa técnica que hace seguimiento a la Política de Seguridad Digital se enfocará en de la Implementación del Modelo de Seguridad y Privacidad de Información – MSPI en la Entidad.

# ALCANCE PLAN MSPI

Establecer la hoja de ruta para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI que es aplicable a todos los procesos de la Entidad; funcionarios, contratistas, lo cual comprende las políticas, procesos, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información.

# OBJETIVO PLAN MSPI

Establecer las actividades contempladas en el MSPI alineadas con la norma técnica ISO 27001, definir acciones lineamientos necesarios para fortalecer la seguridad de la información y garantizar la disponibilidad, integridad y confidencialidad de esta dentro de la Entidad, a partir de las definiciones dadas por el Modelo de Seguridad y Privacidad de la Información - MSPI, la norma técnica ISO 27001 y el Modelo Integrado de Planeación y Gestión- MIPG.

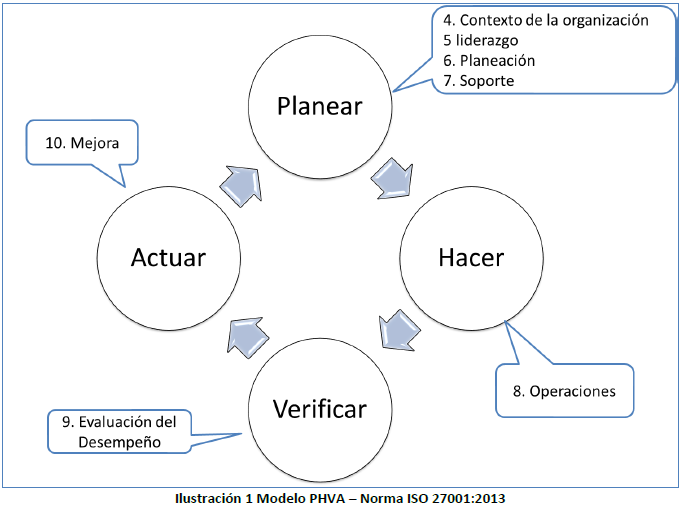
# Objetivos Específicos Plan MSPI

* Definir, actualizar, excluir controles o elementos normativos para proteger la información de la Entidad frente a los criterios de confidencialidad, integridad y disponibilidad.
* Implementar la metodología de Administración y Gestión de Riesgos con el fin de mitigar el impacto en una posible materialización de un riesgo.
* Implementar el plan de comunicaciones del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información fortaleciendo la Entidad.
* Adelantar revisiones del Sistema de Seguridad de Información con el fin de verificar el funcionamiento de este
* Definir los procesos para mejora continua del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información.
* 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.

# 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 ISO 27001-2013

# PLANEAR

En esta primera fase se realiza un estudio de la situación actual de la UAESP, desde el punto de vista de la seguridad 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 (Confidencialidad, integridad y disponibilidad), e igualmente, no toda la información está sometida a los mismos riesgos. Por ello, una de las actividades importantes 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 de Servicios Públicos- UAESP.

En este sentido, se tiene el documento “Análisis de Contexto”, que permite tener una idea clara de la entidad con mayor profundidad, el cual hace parte del MSPI-SGSI de la entidad.

# Políticas 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 directivos, funcionarios, usuarios y terceros que accedan a la información de la Entidad, usen equipos informáticos y de comunicaciones, interactúen con herramientas tecnológicas y/o servicios informáticos y/o ingresen de manera física o lógica a las instalaciones de la Unidad.

La ruta en la página web es la siguiente:

<http://www.uaesp.gov.co/transparencia/planeacion/planes> , realizar click en [Manual de Políticas de Seguridad de la Información](http://www.uaesp.gov.co/transparencia/planeacion/planes/manual-pol%C3%ADticas-seguridad-la-informaci%C3%B3n).

Se elabora el documento Políticas de Seguridad de la Información para dar cumplimiento con algunos controles del anexo A de la norma ISO 27001 de acuerdo con los lineamientos ahí definidos y mediante la resolución 589 de 2019 "Por la cual se adopta la Política de Seguridad de la Información en la Unidad Administrativa Especial de Servicios Públicos"

La ruta en la página web es la siguiente:

<http://www.uaesp.gov.co/sites/default/files/Politica%20de%20Seguridad%20de%20la%20Informacion.pdf>

# 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, el área encargada de realizar, actualizar, hacerle seguimiento y control al Inventario de Activos de Información es la Oficina TIC.

Las actividades por realizar para obtener un inventario de activos son Definición, Revisión, Actualización y Publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información:

* + - 1. **Definición**

Los activos de información que se gestionan en todos los procesos de la Entidad deben cumplir con lo siguiente:

* Número consecutivo único que identifica al activo en el inventario.
* Proceso al que pertenece el activo.
* Propietario / Responsable
* Custodio.
* Nombre del activo de información.
* Descripción del activo de información.
* Categorización del activo de información: por ejemplo, hardware, software, servicio, personas, la cual debe revisarse periódicamente o cuando se presenten cambios en la información o en la estructura que puedan afectarla.
* Idioma.
* Medio de conservación.
* Periodicidad o de generación o actualización en caso de activos expedientes físicos y digitales.
* Condición legitima de la excepción (Ley 1712 transparencia y Ley 1581 tratamiento de datos).
* Fundamento constitucional o legal.
* Descripción de Condición legitima de la excepción.
* Clasificación del activo de acuerdo a la ley de transparencia.
* Valoración del activo (confidencialidad, integridad y disponibilidad).
  + - 1. **Revisión**

El inventario de activos puede ser revisado o validado en cualquier momento que se requiera y por lo menos debe revisarse y actualizarse una vez al año, con el fin de validar el estado del activo, el proceso al que pertenece, cambio o aumento de actividades, desaparición de un área o proceso, cambios o migraciones de sistemas de información del proceso entre otros.

La Entidad a finales de 2019 realizó la actualización del inventario de activos de la información en todos los procesos.

* + - 1. **Actualización**

Cuando el propietario del activo o el líder del Proceso defina alguno de los cambios mencionados anteriormente en los activos de información, se debe actualizar el inventario de activos de información.

* + - 1. **Publicación**

La Entidad, determina que el inventario de activos de información es un documento clasificado como “Público”, sin embargo, aquellos activos de información que por su carácter reservado y que son de naturaleza sensible a los procesos estratégicos de la Entidad, serán clasificados como “Confidenciales”, por lo cual no serán publicados.

El líder de cada proceso será el responsable del inventario de activos de seguridad de la información y las modificaciones que se requieran solo se deben hacer previa autorización del Oficial de Seguridad de la Información o quien haga sus veces.

La ruta en la página web es la siguiente:

<http://www.uaesp.gov.co/transparencia/instrumentos-gestion-informacion-publica/registro-activos-informacion-uaesp>

# Análisis de Brecha

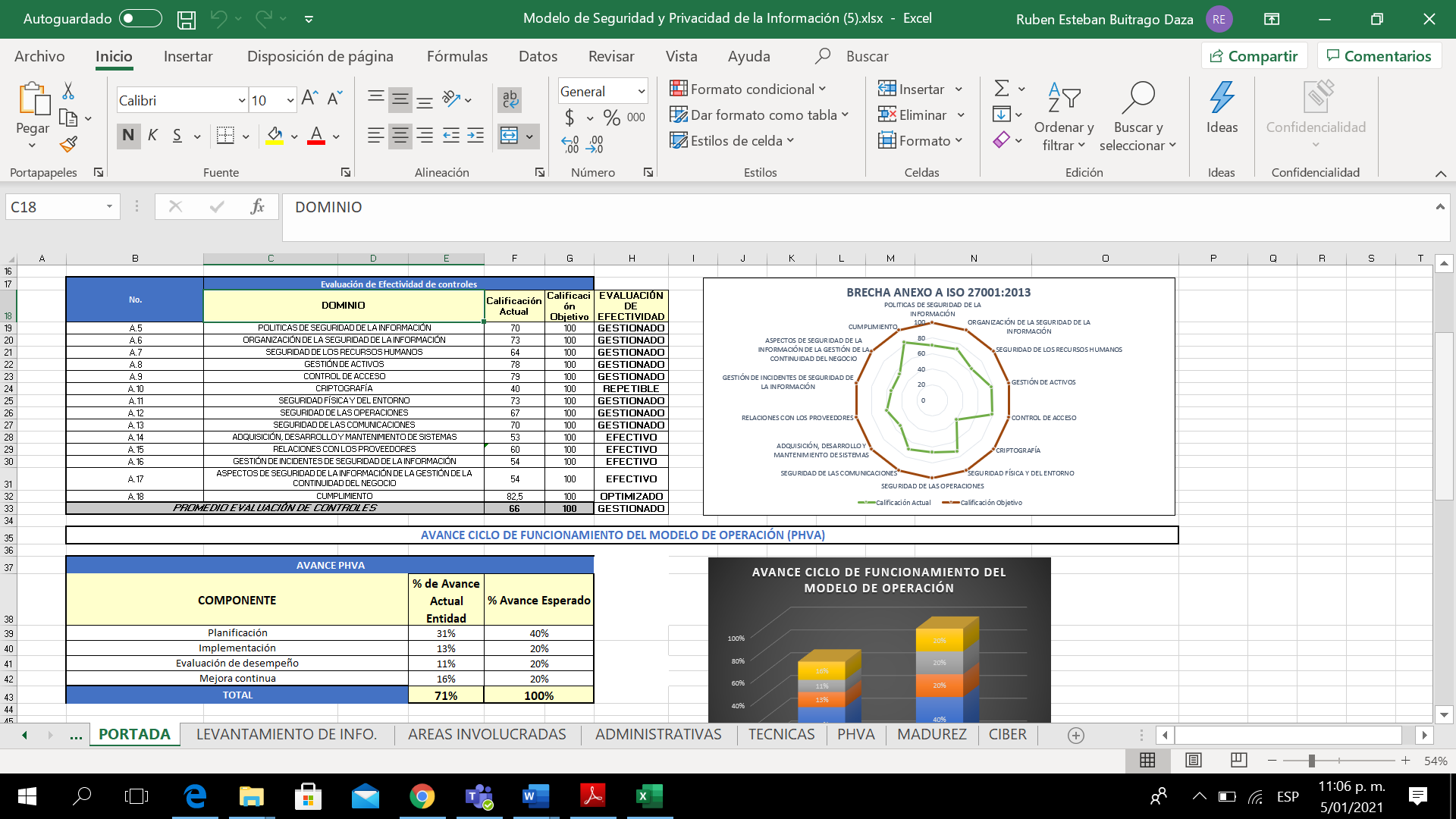
El análisis de brecha busca generar un diagnóstico relativo a la seguridad de la información basado en la identificación de diferencias entre el estado actual y el estado ideal de la Unidad Administrativa Especial de Servicios Públicos de acuerdo con los requerimientos exigidos en la norma ISO 27001:2013, 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.

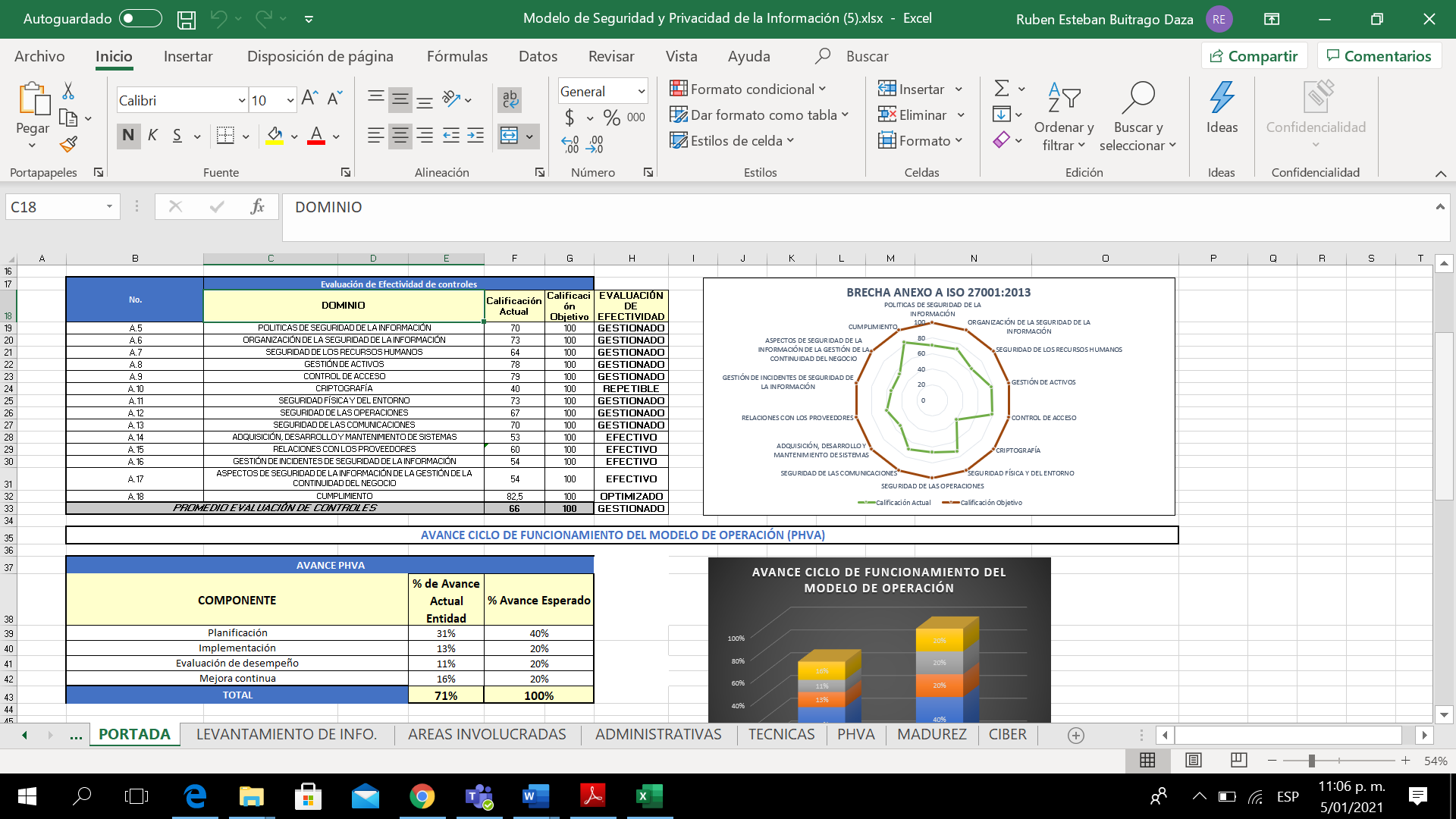
Las fases para realizar una metodología de diagnóstico de seguridad de la información son:

* Revisión del cumplimiento de las exigencias de la Norma ISO 27001 en concordancia con el modelo de seguridad y privacidad de la Información - MSPI, 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 faltantes (Políticas, procedimientos, controles), los cuales son exigidos por la norma ISO 27001 y por el modelo del MinTic – MSPI.

En cumplimiento con lo establecido por el MINTIC, se va a usar la herramienta de autodiagnóstico de seguridad y privacidad de la información elaborada por ellos, la cual arroja un resultado que permite a cada entidad visualizar los diferentes dominios de la norma, evaluar las falencias y a partir de eso, generar un plan de seguridad de la información para ser desarrollado al interior de la misma 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 septiembre de 2020, se generaron los siguientes resultados:

Ilustración 2 Autodiagnóstico MSPI





Fuente: Propia

# Documentación de Procedimientos

Durante esta fase se identificarán y documentarán procedimientos necesarios para dar cumplimiento a la norma ISO 27001 y a las necesidades propias que la entidad requiere, garantizando un adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información - MSPI. Actualmente el proceso de Gestión Tecnológica y de la Información cuenta con los siguientes procedimientos dentro del Sistema Integrado de Gestión:

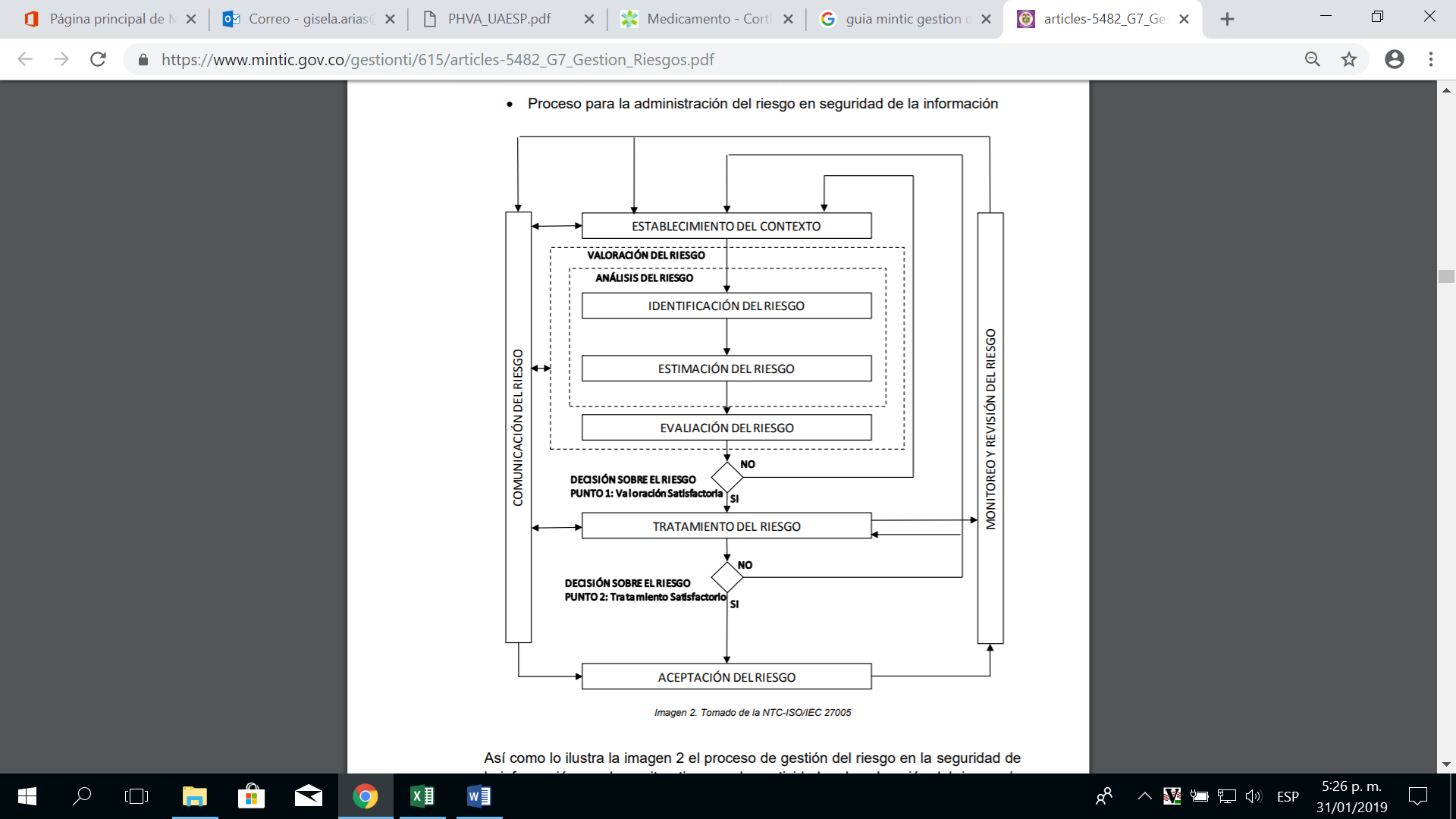
* PC-02 Datos AbiertosV1
* PC-03 Administración de Gestión de Usuarios V5
* PC-04 Activos de Información V1
* PC-05 Mantenimiento y soporte V5
* PC-06 Administración Servidores V2
* PC-07\_Administracion\_Comunicaciones\_Tecnologica\_Informacion V3
* PC-08 Administración de Hardware V1
* PC-09 Administración Software V1
* PC-10 Administración de Antivirus V1
* PC-11 Generación de Backups en servidores V1
* PC-12 Generación de Backups de Equipos de Cómputo V1
* PC-13 Cifrado de la Información V1
* PC-14 Dispositivos Móviles V1
* IN-01Presentación soportes información para cobro V1
* IN-02 Análisis de Vulnerabilidades o Pentest V1

En este sentido, la entidad entra a valorar cada uno de los procedimientos con el fin de hacer la revisión desde la perspectiva del SGSI-MSPI, acoplarlos a las nuevas necesidades y crear los nuevos procedimientos que permitan dar cumplimiento a los controles definidos por la norma y por el quehacer de la entidad.

# Metodología para la Gestión de Riesgos

La gestión de riesgos de seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento, el cual es adoptado desde la Oficina Asesora de Planeación como Política de gestión de Riesgos y el SGSI – MSPI se une a dichos dictámenes que acoplan el Modelo de Riesgos definidos por el Departamento Administrativo de la Función Pública – DAFP a la Entidad. En ese sentido y de forma ilustrativa, se visualiza el siguiente gráfico con el fin de esquematizar de manera somera el proceso descrito por la entidad:

Ilustración 3. Administración del riesgo en seguridad de la información



Fuente: NTC-ISO/IEC 27005

Así como lo ilustra la imagen anterior, la gestión del riesgo es iterativo para las actividades de valoración del riesgo y/o el tratamiento de este. Un enfoque iterativo para realizar la valoración del riesgo incrementa la profundidad y el detalle de la valoración en cada iteración y obliga a un proceso de mejora continua como se está proponiendo dentro de este sistema.

La gestión de riesgos ofrece a la UAESP un método sistemático para analizar los riesgos derivados de los procesos y del uso de las tecnologías de la información y comunicaciones,

con el objetivo de descubrir y planificar el tratamiento oportuno, mantener los riesgos bajo control y así preparar a la entidad para un proceso de evaluación, auditoría, certificación o acreditación, según corresponda.

La información adoptada por la Entidad referente a dicha metodología es presentada en la **Matriz Identificación riesgos seguridad de la información.xlsl**

# Programas de Sensibilización y/o Formación de Empleados

El documento ***Plan de Sensibilización*** presenta la planeación para realizar el programa de sensibilización y/o formación sobre Seguridad de Información dentro de la Entidad, el cual tiene como objetivos principales, lograr que los miembros que integran la UAESP, entiendan y se comprometan con todos los aspectos relacionados con el Sistema de Gestión de Seguridad de la Información, a partir de la creación de una cultura relacionada con la integridad, confidencialidad y disponibilidad de la información, en donde todos los miembros de la entidad comprendan la importancia de dar un tratamiento adecuado a la información y finalmente concientizar a las personas de los riesgos que se pueden presentar tanto para ellas como parte integral de UAESP y su misión social, como para la imagen pública de la entidad.

# Gestión de los Recursos del SGSI-MSPI

Es compromiso de la Dirección de la UAESP, el garantizar los recursos tanto presupuestales como del talento humano para la implementación exitosa del SGSI - MSPI.

# Soporte

# Recursos

La Alta Dirección con el apoyo de la Oficina de Tecnología de la Información y las Comunicaciones deben planificar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de la Seguridad de la Información.

# Competencia

La competencia significa la capacidad con la que se aplican los conocimientos y las habilidades en la Entidad con el fin de conseguir los resultados previstos en cuanto a la implementación del Sistema de Gestión de la Seguridad de la Información.

A continuación, se describen las siguientes competencias:

Tabla 1: Competencias

|  |  |
| --- | --- |
| **PERFIL** | **COMPETENCIAS** |
| Comité Institucional de Gestión y Desempeño | **1)** Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión - MIPG.  **2)** Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión - MIPG.  **3)** Proponer al Comité Sectorial de Gestión y el Desempeño Institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG.  **4)** Presentar los informes que el Comité Sectorial de Gestión y el Desempeño Institucional y los organismos de control requieran sobre la gestión y el desempeño de la entidad.  **5)** Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión.  **6)** Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.  **7)** Las demás que tengan relación directa con la implementación, desarrollo y evaluación del Modelo. |
| Jefe de TIC | **1)** El jefe de TIC tiene la responsabilidad global del suministro y uso de las TIC en la Entidad.  **2)** Debe Organizar y supervisar el trabajo de un equipo de personas especializadas que son las encargadas de diferentes tareas en cuanto a la implementación y seguimiento del SGSI-MSPI.  **3)** Respetar y cumplir los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). |
| Encargado de Infraestructura | **1)** Garantizar la definición, monitoreo, accesibilidad, funcionalidad y mantenimiento de las redes y servidores del Entidad.  **2)** Colaborar en la correcta ejecución y control de los procesos de creación de respaldos de información y/o recuperación.  **3)** Registrar y controlar el inventario de infraestructura de la de la Dirección de Tecnologías de Información y Comunicación.  **4)** Supervisar el correcto funcionamiento de la plataforma tecnológica de la Entidad a través de sistemas de monitoreo, a fin de prevenir interrupciones en el servicio y gestionar las acciones que permitan garantizar su adecuado funcionamiento. |
| Personal de la UAESP | **1)** Respetar y seguir las normas y procedimientos definidos en la política de seguridad de la información.  **2)** Notificar al responsable de seguridad de la información las anomalías o incidentes de seguridad, así como las situaciones sospechosas.  **3)** Mantener la confidencialidad, integridad y disponibilidad de la información.  **4)** Hacer un buen uso de los activos de información de la Entidad. |

# Toma de Conciencia

La Oficina de Tecnologías de información y las Comunicaciones, adelantará un plan de sensibilización y/o formación por diferentes medios, buscando que todos y cada uno de los funcionarios, contratistas y partes interesadas, se enteren de la implementación del MSPI-SGSI, sus pormenores y sobre todo de la labor que cada uno de ellos adelanta dentro de la entidad, haciendo especial énfasis en las responsabilidades de cada uno y los posibles problemas que recaen sobre ellos o la entidad, en el caso del incumplimiento de las políticas de Seguridad de Información.

# Comunicación

La entidad tiene definido un procedimiento para manejo de incidentes de seguridad, el cual plantea actividades específicas orientadas a la comunicación de dichos incidentes a las partes interesadas.

# Información Documentada

La Entidad, dentro de la implementación del MSPI-SGSI, adelantará el registro y documentación de los requerimientos exigidos por la norma ISO27001:2013 y los documentos adicionales definidos por el MSPI, llevando a cabo el versionamiento solicitado por la norma y alineado a los procedimientos definidos por la oficina de Planeación para llevar a cabo este tipo de tareas.

# HACER

# Operación



En esta fase se lleva a cabo el establecimiento de los controles de seguridad escogidos en

la fase anterior junto con los seguimientos, actualizaciones y procesos de mejora propios. Dentro de esta fase se destaca el cumplimiento del plan de sensibilización, que conlleva a la concientización y/o formación del personal de la UAESP de cara a que conozcan los controles implantados, el rol que cada funcionario, contratista o parte interesada desempeña y sobre todo el buscar la colaboración de cada una de las personas como parte activa del sistema.

Dichos controles se especifican en el documento **Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Matriz Identificación Riesgos Seguridad de la Información.**

# Métricas de Eficacia de los Controles y del Sistema.

Toda vez que el SGSI-MSPI es un sistema de mejora continua, hay necesidad de definir parámetros precisos para evaluar los controles ejecutados 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 este.

# Gestión de Funcionamiento normal 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 continuo 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 suplir 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 implementa un ***Plan de Gestión de Incidentes,*** creado para detectar y gestionar un incidente, definido como toda aquella actividad ejecutada como resultado de eventos adversos e inesperados que ocurran como resultado de controles fallidos o inexistentes, teniendo en cuenta las directrices adelantadas por MINTIC, la Policía Nacional y los entes competentes en esta área.

# VERIFICAR

# Evaluación de Desempeño

La UAESP dispone de mecanismos que le permitan 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 en el MSPI 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 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 implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se realiza su respectivo.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **GESTIÓN** | **ACTIVIDADES** | **TAREAS** | **RESPONSABLE DE LA TAREA** | **FECHAS PROGRAMACIÓN TAREAS** |
| Activos de Información | Definir lineamientos para el levantamiento de activos de información | Actualización de metodología e instrumento de levantamiento de activos de información | Juan Perdomo | 30 de enero de 2021 |
| Levantamiento Activos de Información | Socializar la guía de activos de Información. | Rubén Buitrago  Grupo MSPI | 1 junio de 2021 |
| Validar activos de información en el instrumento levantado en la vigencia anterior | Rubén Buitrago  Grupo MSPI | 1 junio de 2021 |
| Publicación de Activos de Información | Validar y aceptar los activos de información para su publicación en la Página Web por cada líder de proceso. | Rubén Buitrago  Grupo MSPI | 2 semestre de 2021 |
| Registros activos de información ley 1712 | Actualizar el instrumento de Registro Activos de Información con el insumo de los instrumentos de activos de Información. | Rubén Buitrago  Grupo MSPI | 30 de enero de 2021 |
| Reporte Datos Personales | Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos. | Rubén Buitrago  Grupo MSPI | 1 junio de 2021 |
| Gestión de Riesgos | Actualización de lineamientos de riesgos | Actualizar plan de tratamiento de riesgos de seguridad de la Información | Osbaldo Cortes | 28 de febrero de 2021 |
| Sensibilización | Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital. | Osbaldo Cortes  Grupo MSPI | 28 de febrero de 2021 |
| Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital. | Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital. | Osbaldo Cortes  Grupo MSPI | 28 de febrero de 2021 |
| Realimentación, revisión y verificación de los riesgos identificados (Ajustes) | Osbaldo Cortes  Grupo MSPI | 28 de febrero de 2021 |
| Aceptación de Riesgos Identificados | Aceptación, aprobación Riesgos identificados y planes de tratamiento de Riesgos | Osbaldo Cortes  Grupo MSPI | 28 de febrero de 2021 |
| Publicación | Actualizar Matriz de riesgos | Osbaldo Cortes  Grupo MSPI | 28 de febrero de 2021 |
| Gestión de Incidentes de Seguridad de la Información | Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información | Elaboración y publicación del procedimiento de incidentes de seguridad de la información | Juan Perdomo  Grupo MSPI | 1 abril de 2021 |
| Socializar el procedimiento al talento humano de la Oficina TIC. | Juan Perdomo  Grupo MSPI | 1 abril de 2021 |
| Socializar el procedimiento funcionarios y Contratistas de la Entidad. | Juan Perdomo  Grupo MSPI | 15 de abril de 2021 |
| Gestionar los incidentes de Seguridad de la Información identificados | Gestionar los incidentes de Seguridad de la Información identificados | Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido. | Juan Perdomo  Osbaldo Cortes  Oscar Rodríguez | Continuo en la Vigencia |
| CSIRT | Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno | Fabian Lozano | Continuo en la Vigencia |
| Eventos/vulnerabilidades | Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI | Osbaldo Cortes  Grupo MSPI | Continuo en la Vigencia |
| Plan de Continuidad del Negocio | Documentación del Análisis de Impacto de la Operación | Elaboración del Análisis de Impacto del Negocio | Paola Nova  Grupo MSPI | 1 de junio de 2021 |
| Publicación del Análisis de Impacto del Negocio | Paola Nova  Grupo MSPI | 1 de agosto de 2021 |
| Documentación de Valoración de Riesgos de Interrupción | Actualización del documento Valoración de Riesgos de interrupción para el plan de operación | Paola Nova  Grupo MSPI | 1 de junio de 2021 |
| Documentación del Plan de continuidad de la Operación | Aprobación del Plan de continuidad de la Operación | Paola Nova  Grupo MSPI | 1 de agosto de 2021 |
| Gobierno Digital | Gobierno Digital | Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información. | Grupo MSPI | 31 de enero de 2021 |
| Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente. | Grupo MSPI | Continuo en la Vigencia |
| Auditorías Internas y Externas | Participación en las auditorías internas y externas de la norma ISO 27001:2013 | Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas en el PAAI | Paola Nova | Continuo en la Vigencia |
| Revisión de los controles de la norma ISO 27001:2013 | Revisión de los controles de la norma ISO 27001:2013, | Revisar y actualizar la Matriz de Riesgos y la Matriz Autodiagnóstico del MSPI. | Grupo MSPI | 1 de mayo de 2021 |
| Indicadores SGSI | Provisión de información a los indicadores de medición del SGSI | Formular, Implementar, actualizar y reportar los indicadores del SGSI | Juan Perdomo | 1 de diciembre de 2021 |
| Vulnerabilidades |  | Revisión y actualización del instructivo Análisis de Vulnerabilidades | Osbaldo Cortes  Fabian Lozano | 1 de mayo de 2021 |
| Protección de datos personales | Recolectar bases de datos | Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC | Gisela Arias  Grupo MSPI | 15 de febrero de 2021 |
| Revisión de bases de datos | Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos | Gisela Arias  Grupo MSPI | 15 de junio de 2021 |
| Registro y actualización de las bases de datos | Registrar o actualizar las bases de datos en la plataforma de la SIC teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información | Gisela Arias  Grupo MSPI | 1 de agosto de 2021 |
|  | Verificar Matriz Autodiagnóstico | Actualización, seguimiento y monitoreo de los dominios del autodiagnóstico MSPI. | Grupo MSPI | 30 de enero de 2021 |

Tabla 2: Plan de implementación