

**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**Bogotá, D.C.,**

**DICIEMBRE DE 2020**

CONTENIDO

[1. INTRODUCCION 4](#_Toc59209305)

[2. OBJETIVOS 5](#_Toc59209306)

[2.1. GENERAL 5](#_Toc59209307)

[2.2. ESPECIFICOS 5](#_Toc59209308)

[3. ALCANCE 5](#_Toc59209309)

[4. GLOSARIO 6](#_Toc59209310)

[4.1. SIGLAS 7](#_Toc59209311)

[5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8](#_Toc59209312)

[6. CICLO DE OPERACIÓN 8](#_Toc59209313)

[7. FASE DE DIAGNOSTICO. 9](#_Toc59209315)

[7.1. Ciclo de funcionamiento del modelo de operación (PHVA). 10](#_Toc59209317)

[7.2. ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN. 11](#_Toc59209318)

[7.3. Desempeño de mejores prácticas en Ciberseguridad (NIST). 13](#_Toc59209320)

[7.3.1. Identificar. 13](#_Toc59209321)

[7.3.2. Proteger. 14](#_Toc59209322)

[7.3.3. Detectar. 14](#_Toc59209323)

[7.3.4. Responder. 15](#_Toc59209324)

[7.3.5. Recuperarse. 15](#_Toc59209325)

[8. FASE DE PLANIFICACION 16](#_Toc59209326)

[9. FASE DE IMPLEMENTACION. 17](#_Toc59209328)

[10. FASE DE EVALUACIÓN DE DESEMPEÑO. 17](#_Toc59209330)

[11. FASE DE MEJORA CONTINUA. 18](#_Toc59209332)

[12. METODOLOGIA. 19](#_Toc59209334)

[13. RECURSOS 21](#_Toc59209336)

[14. MAPA DE RUTA. 22](#_Toc59209337)

ILUSTRACIONES

[Ilustración 1. Ciclo de Operación. 9](#_Toc56669587)

[Ilustración 2. Fase de Diagnóstico MSPI. 9](#_Toc56669589)

[Ilustración 3. Alineación norma ISO 27001:2013 al Ciclo Mejora Continua. 12](#_Toc56669592)

[Ilustración 4. Fase de Planeación MSPI. 16](#_Toc56669600)

[Ilustración 5. Fase de Implementación MSPI. 17](#_Toc56669602)

[Ilustración 6. Fase de Evaluación y Desempeño MSPI. 18](#_Toc56669604)

[Ilustración 7. Fase de Mejora Continua MSPI. 18](#_Toc56669606)

[Ilustración 8. Metodología PHVA. 20](#_Toc56669608)

# **INTRODUCCION**

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

En este modelo se propone un conjunto de guías prácticas que contribuyen a mitigar los riesgos asociados a la seguridad de la información, así como velar por la preservación de la confidencialidad, integridad y disponibilidad de los activos de información con los que cuenta la Entidad. En tal sentido, la seguridad de la información actúa como eje transversal e integral para el desarrollo de objetivos y metas propuestas a través de estructuras de relaciones y procesos organizacionales que velan por la protección de este activo vital de la entidad, por lo que se realizará seguimiento y control cada año o cuando se requiera.

# **OBJETIVOS**

# **GENERAL**

Generar la estrategia para la definición e implementación de políticas, controles, lineamientos, procedimientos y buenas prácticas que contribuyan con la preservación de la disponibilidad, integridad y confidencialidad de los activos de información.

# **ESPECIFICOS**

* Promover el uso de mejores prácticas de seguridad de la información como base de aplicación del concepto de Seguridad Digital.
* Establecer los procedimientos, controles y buenas prácticas para la gestión de eventos e incidentes que afecten la integridad, confidencialidad e integridad de los activos de información de la entidad.
* Definir políticas y controles que contribuyan con la seguridad de la información de la entidad.
* Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
* Cumplir con los principios de seguridad de la información.
* Apoyar e impulsar la innovación tecnológica en la Entidad.
* Velar por la gestión de continuidad del negocio frente a incidentes de seguridad de la información.
* Fortalecer el desarrollo del ejercicio de Arquitectura Empresarial de la entidad, mediante la identificación e incorporación de controles y procesos para asegurar la seguridad y privacidad de la información.
* Sensibilizar el talento humano para la gestión eficiente y eficaz en seguridad de la información.

## **ALCANCE**

Este plan aplica a todos los procesos de la Unidad Administrativa Especial De Rehabilitación Y Mantenimiento Vial, como a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la Entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que acceden, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica sobre toda la información creada, procesada o utilizada por la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, sin importar el medio, formato, presentación o lugar en el cual se resguarde.

## **GLOSARIO**

* **Activos de Información:** Cualquier elemento de información o que interactúe con ella y que sea necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo.
* **Ciberseguridad:** la ciberseguridad se define como una **capa de protección para los archivos de información**, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.
* **Confidencialidad:** La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
* **Correlacionador de Eventos:** Un correlacionador de eventos de seguridad, también conocido como SIEM (Security Information and Event Management), tiene como objetivo principal el ayudar a las empresas a construir un centro de operaciones de seguridad en donde se tenga centralizada la información de múltiples fuentes y además brinde la posibilidad de identificar ataques complejos que afectan múltiples puntos a la vez
* **Disponibilidad:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.
* **Evento de seguridad de la información**: un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la
* **Impacto**: Es un efecto que ocurre a causa de la materialización de un riesgo y que va en detrimento de uno o más de los recursos importantes del negocio (Recursos: Financiero, Imagen, Ambiental, Humano, entre otros).
* **Incidente de Seguridad:** Según la norma ISO 27035, un Incidente de Seguridad de la Información es indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.
* **Integridad:** La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.
* **Riesgo**: Es la definición de un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio (por ejemplo, pérdida de la continuidad, incumplimiento, pérdida de ingresos, entre otros).
* **Seguridad de la Información:** Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.
* **Sistema de Detección de Intrusos:** Un Sistema de Detección de Intrusos (IDS: Intrusion Detection System) es un componente dentro del modelo de seguridad informática de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómala, desde el exterior o interior de un dispositivo o una infraestructura de red.
* **Vulnerabilidad**: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de una organización.

## **SIGLAS**

* **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
* **MSPI:** Modelo de Seguridad y Privacidad de la Información.
* **NIST:**National Institute of Standards and Technology.
* **IPV4:** Internet Protocol Versión 4.
* **IPV6:** Internet Protocol Versión 6.
* **UAERMV:** Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

## **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

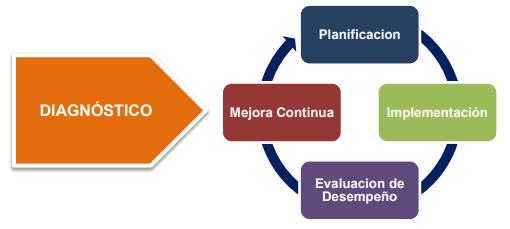
La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para dar cumplimiento a lo establecido en el Decreto 1078 del 26 de mayo de 2015 del MinTIC: por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, inició la implementación del Modelo de Seguridad y Privacidad de la Información-MSPI. La adopción y aplicación, tiene contemplado un ciclo de operación que consta de cinco (5) fases, las cuales permiten que la entidad pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC, para la Gestión al aportar en el uso estratégico de las tecnologías de la información, con la formulación e implementación del modelo de seguridad, enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

## **CICLO DE OPERACIÓN**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, va a desarrollar el habilitador seguridad y privacidad de la información, utilizando la metodología definida por el MinTIC, haciendo uso en las guías para la implementación del modelo de seguridad y privacidad de la información-MSPI, que establece cinco fases a través de un ciclo de operación con objetivos, metas y actividades que se mencionan a continuación:

## **Ilustración 1. Ciclo de Operación.**

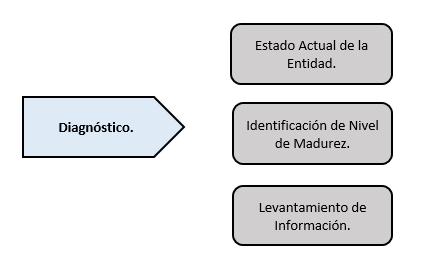


**Fuente: Guía Modelo de Seguridad y Privacidad de la Información - MINTIC.**

La ilustración 1 muestra que se inicia el ciclo de operación a partir del diagnóstico, posteriormente al diagnóstico se establecen cuatro fases, las cuales son las encargadas de gestionar la protección de los activos de información, los riesgos asociados a los activos y finalmente las que dan cumplimiento a los requisitos de Ley.

## **FASE DE DIAGNOSTICO.**

## **Ilustración 2. Fase de Diagnóstico MSPI.**



**Fuente: Modelo de Seguridad y Privacidad de la Información.**

Determinar el nivel de madurez y cumplimiento actual acerca de la gestión de la seguridad de la información realizada al interior de la entidad, para lo cual se utiliza el instrumento diseñado por el MINTIC denominado “Instrumento de Evaluación MSPI”, el cual contribuye a identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de la Entidad.

Por medio de este instrumento, se permite establecer el porcentaje de avance del modelo de operación (PHVA), el cual contribuirá a la mejora continua de cada una de las fases dentro del ciclo de operación del MSPI, adicional permite identificar el nivel de madurez actual sobre los controles y la gestión de riesgos orientados hacia la Ciberseguridad, tomando como referente el estándar NIST 800-53, donde se obtienen los siguientes resultados:

* Evaluación de efectividad de controles - ISO 27001:2013 anexo A.

El anexo A del estándar internacional ISO 27001:2013 se especifican 14 dominios, 35 objetivos de control y un total de 114 controles, los cuales pretenden mitigar los riesgos y realizar una adecuada gestión de la seguridad de la información.

Debido a lo mencionado anteriormente, los resultados obtenidos en el instrumento de diagnóstico, permitirán determinar, la escala de evaluación de los controles relacionados con los dominios de la norma ISO27001:2013, estas evaluaciones logran identificar cuando un control no se aplica oportunamente o si la forma en que se aplica el control no es la más precisa o indicada. De esta manera este ejercicio permite orientar los esfuerzos de la entidad para fortalecer los controles de la norma ISO 27001:2013.

## **Ciclo de funcionamiento del modelo de operación (PHVA).**

Se conoce como PHVA al ciclo de cuatro (4) fases definidas como Planear, Hacer, Verificar y Actuar, que de manera sistémica operan en función de lograr el mejoramiento continuo acerca de los productos o servicios que ofrecen las distintas organizaciones. Para tal fin, la entidad luego de aplicar el formato Instrumento de Evolución MSPI, logra determinar el nivel de cumplimiento del ciclo definido dentro del MSPI de la siguiente manera:

* + 1. **Fase de Planificación:**

La entidad ha definido un marco de seguridad y privacidad de la información, dado que actualmente cuenta con: la política de seguridad y privacidad de la información, una serie de procedimientos generales de seguridad, posee un inventario de activos de la información y se tiene documento con la metodología, análisis, evaluación y tratamiento de riesgos. Sin embargo, resulta importante desarrollar la documentación acerca de procedimientos detallados de seguridad de la información, establecer los roles y responsabilidades de Seguridad de la Información, definir el plan de comunicación y sensibilización de SI, realizar la declaración de aplicabilidad, plan de diagnóstico de IPV4 a IPV6, así como fortalecer e implementar el programa de gestión de riesgos de la información de la entidad.

* + 1. **Fase de Implementación:**

En esta fase la entidad ha realizado avances acerca el tratamiento de riesgos, aunque se hace evidente llevar a cabo el plan de tratamiento de riesgos de Seguridad de la información, además definir y aplicar indicadores y métricas acerca de la gestión de la seguridad y privacidad de la información.

* + 1. **Fase de Evaluación de Desempeño:**

Actualmente la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, establecerá un plan de auditorías y un plan de seguimiento, no obstante, el nivel de desarrollo de las etapas anteriores limita los resultados de la evaluación del desempeño en cuanto a la gestión de la seguridad de la información.

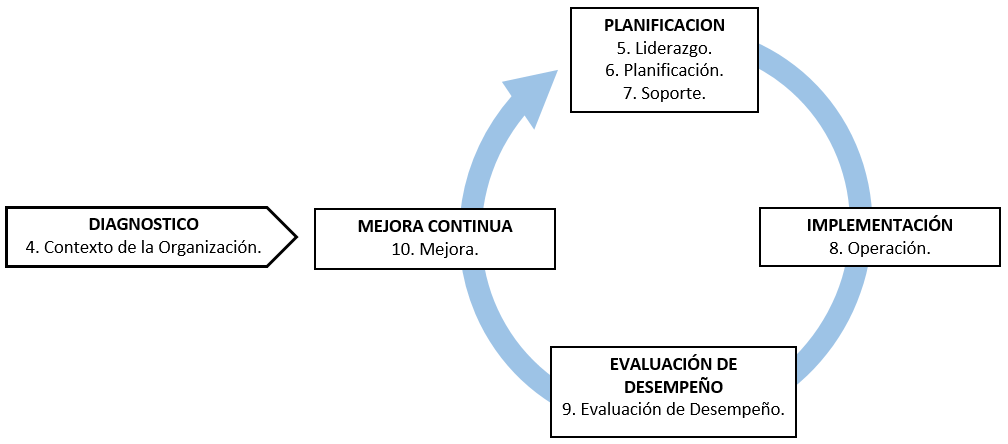
* + 1. **Fase de Mejora Continua:**

Sobre esta fase resulta importante que la entidad avance aún más en las metas y resultados de las fases anteriores de modo que se defina un plan de mejoramiento y un plan para la comunicación de resultados de la gestión e implementación del MSPI.

## **ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACIÓN.**

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

## **Ilustración 3. Alineación norma ISO 27001:2013 al Ciclo Mejora Continua.**



**Fuente: Elaborada en base a la ISO 27001:2013.**

* **FASE DIAGNOSTICO,** en la norma ISO 27001:2013. En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, determina la necesidad de realizar un análisis de las cuestiones externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesadas de la organización en el alcance del modelo de seguridad de la información.
* **FASE PLANEACION,** en la norma ISO 27001:2013. En el capítulo 5 - Liderazgo, establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización, asegure la asignación de los recursos para la seguridad de la información y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

En el capítulo 6 - Planeación, se establecen los requerimientos para la valoración y tratamiento de riesgos de seguridad, y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

En el capítulo 7 – Soporte, se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del modelo de seguridad de la Información.

* **FASE IMPLEMENTACIÓN,** en la norma ISO 27001:2013. En el capítulo 8 - Operación de la norma ISO 27001:2013, indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.
* **FASE EVALUACIÓN DEL DESEMPEÑO,** en la norma ISO 27001:2013. En el capítulo 9 - Evaluación del desempeño, se definen los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.
* **FASE MEJORA CONTINUA,** en la norma ISO 27001:2013. En el capítulo 10 - Mejora, se establece que, para el proceso de mejora del modelo de seguridad de la Información, a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

## **Desempeño de mejores prácticas en Ciberseguridad (NIST).**

De acuerdo con NIST, en el año 2014 la agencia emitió el marco de trabajo “NIST Cybersecurity Framework” que contempla directrices, prácticas y estándares para gestionar de manera adecuada la infraestructura critica de las organizaciones permitiendo una adecuada gestión de los riesgos de seguridad cibernética. El framework se encuentra estructurado con funciones, categorías, subcategorías y referencias informativas que le permiten a la UAERMV realizar una adecuada gestión de la Ciberseguridad en cada una de las funciones de la siguiente manera:

## **Identificar.**

Esta función requiere el desarrollo y comprensión organizacional de la importancia de los activos de información para priorizar esfuerzos en la administración y gestión de los riesgos de Ciberseguridad. Las categorías que hacen parte de esta función, el Framework las denomina como:

* Gestión de activos.
* Gobernanza.
* Ambiente de negocios.
* Evaluación de riesgos.
* Estrategia de gestión de Riesgos.

En este sentido resulta importante priorizar la gestión y clasificación de activos de información, en especial con aquella información que hace parte de la misionalidad y con los objetivos estratégicos, que permita realizar una apropiada evaluación de riesgos y posibles amenazas de Ciberseguridad.

## **Proteger.**

En esta función se desarrollan e implementan medidas de protección que permitan proteger la integridad, confidencialidad y disponibilidad de los datos, información, sistemas de información y servicios tecnológicos. Adicionalmente, esta función debe medir la capacidad de los recursos frente a eventos e incidentes de Ciberseguridad, por lo tanto, resulta importante llevar una adecuada gestión en las siguientes categorías:

* Control de acceso.
* Capacitación y sensibilización.
* Seguridad de los datos.
* Procesos y procedimientos de protección de la información.
* Mantenimiento.
* Tecnología de protección.

Sobre esta función se hace necesario que la UAERMV fortalezca actividades, controles, procesos y procedimientos de seguridad cibernética de forma continua, permitiendo así alcanzar niveles de protección adecuados sobre los activos críticos de la entidad, y de esta forma lograr reducir el nivel de exposición al riesgo que se enfrentan.

## **Detectar.**

En la detección se emplean mecanismos de prevención y detección oportuna acerca de eventos e incidentes de seguridad de la información, que puedan afectar las infraestructuras tecnológicas y demás activos críticos para la entidad y para ello, son contempladas las siguientes categorías:

* Anomalías y eventos.
* Monitoreo continuo de la seguridad.
* Procesos de detección.

La entidad posee algunos recursos que apoyan la identificación de anomalías y eventos, es necesario contar con herramientas tecnológicas de seguridad como: talento humano capacitado, procesos estandarizados, herramientas para la prevención de fuga de información, sistemas de prevención y detección de intrusos, herramientas de análisis de vulnerabilidades, correlacionador de eventos, herramientas para la protección de aplicaciones web, entre otros, que de manera articulada detecten oportunamente riesgos, amenazas, eventos e incidentes.

## **Responder.**

La función de responder se encarga de llevar a cabo el despliegue de procesos, procedimientos, recursos tecnológicos y talento humano para responder ante la materialización de eventos de seguridad cibernética con el propósito de lograr un impacto bajo sobre los activos de información de las organizaciones. Para esto, es necesario adoptar las siguientes categorías:

* Planes de respuesta a eventos e incidentes.
* Comunicaciones.
* Análisis.
* Mitigación.
* Mejoras (Procesos, Tecnología, Talento Humano).

## **Recuperarse.**

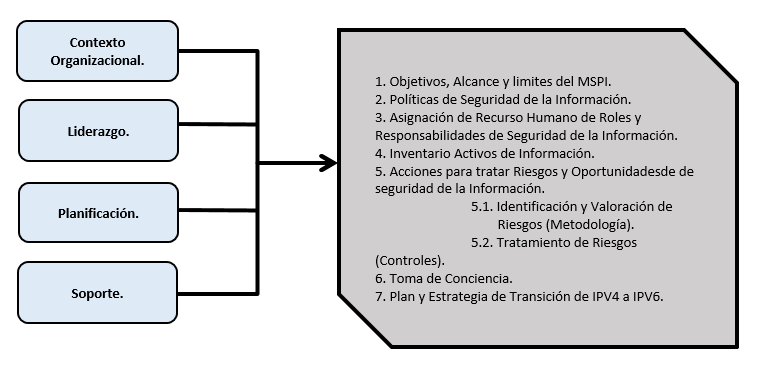
En esta función las actividades están asociadas para que las organizaciones cuenten con un plan de contingencia, plan de recuperación de desastres y plan de continuidad de negocio, para retornar a la operación y funcionamiento normal luego de un incidente, con el objetivo de reducir el impacto. Por lo tanto, es necesario contemplar las siguientes categorías:

* Planes de recuperación.
* Mejoras.
* Comunicaciones.

Actualmente en la entidad se depende en gran medida de la experticia, conocimientos y formación del talento humano. Por lo que se evidencia una problemática inmediata que atender a nivel general sobre cada una de las funciones que contribuyan a la gestión de la seguridad y privacidad de la información.

## **FASE DE PLANIFICACION**

## **Ilustración 4. Fase de Planeación MSPI.**



**Fuente: Modelo de Seguridad y Privacidad de la Información.**

En esta fase se recopila la información de la fase de diagnóstico y se determinan las actividades que han sido realizadas.

* Definición y adopción de las políticas de seguridad de la información.
* Definir roles y responsabilidades de seguridad de la información.
* Inventario de activos de información.
* Identificación y análisis de vulnerabilidades sobre la infraestructura tecnológica.
* Identificación y valoración de riesgos de seguridad digital.
* Definición de procedimientos de seguridad de la información.
* Definición guía para la gestión de incidentes de seguridad de la información.

## **FASE DE IMPLEMENTACION.**

## **Ilustración 5. Fase de Implementación MSPI.**



**Fuente: Modelo de Seguridad y Privacidad de la Información.**

En esta fase se lleva a cabo la implementación de la fase de planificación realizada, en donde se alcanzarán los siguientes logros:

* Definición e implementación de controles contemplados para el tratamiento de riesgos de seguridad digital.
* Gestionar los eventos e incidentes de seguridad de la información.

## **FASE DE EVALUACIÓN DE DESEMPEÑO.**

## **Ilustración 6. Fase de Evaluación y Desempeño MSPI.**



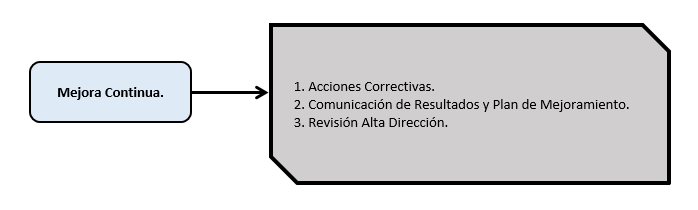
**Fuente: Modelo de Seguridad y Privacidad de la Información.**

En la fase de evaluación de desempeño se realiza seguimiento y monitoreo al MSPI, tomando de referencia los indicadores y métricas estratégicas, estratégicas y operativas que apoyen la posterior toma de decisiones sobre el MSPI, en donde se alcanzarán los siguientes logros:

* Seguimiento a la implantación del MSPI.
* Realización de auditorías al MSPI.

## **FASE DE MEJORA CONTINUA.**

## **Ilustración 7. Fase de Mejora Continua MSPI.**



**Fuente: Modelo de Seguridad y Privacidad de la Información.**

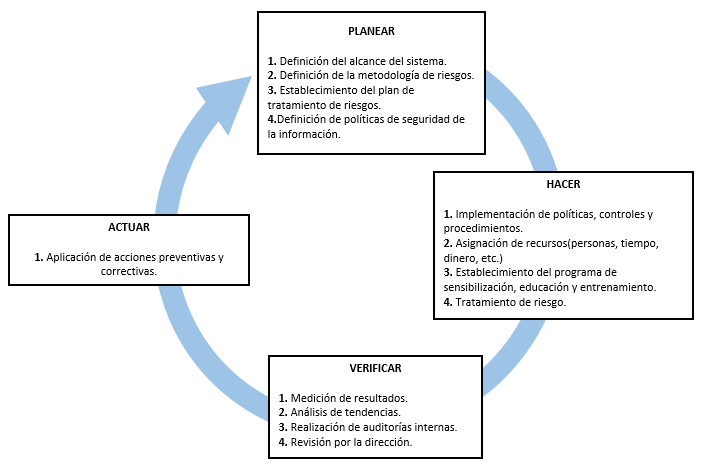
En esta fase se consolidan los resultados de la fase anterior, que sirven de insumo para elaborar el plan de mejoramiento continuo, contemplando las acciones correctivas y preventivas adecuadas, que contribuyan a la eficacia del MSPI, para lo cual aún no se han logrado avances significativos y es necesario realizar las siguientes actividades:

* Desarrollar plan de mejora continua: Durante la vigencia del plan de seguridad y privacidad de la información, se gestionarán las acciones correctivas y preventivas, producto de los seguimientos y revisiones a la implementación, y las auditorias programadas dentro del plan de auditoria de Control Interno.
* Gestión de las comunicaciones de este plan: La adecuada administración de las comunicaciones, permitirán fortalecer las estrategias, para lograr una efectiva comunicación interna y externa de manera transversal, mejorando la gestión en temas de seguridad y privacidad de la información, teniendo en cuenta los siguientes elementos:
  + Información a comunicar: La comunicación contendrá detalles de: avances en las actividades programadas, resultados de los seguimientos al plan, comunicación de atención a incidentes, tips de buenas prácticas de seguridad en la información implementadas en la UAERMV, y su periodicidad se realizará de acuerdo a los avances y las necesidades identificadas por el área de Sistemas o la Dirección de la entidad.
    - * Audiencia identificada: De acuerdo a los objetivos propuestos en el plan, en la audiencia objetivo se describe de la siguiente manera:
    - Público Interno: Son los servidores que trabajan en la entidad ya sea en calidad de funcionarios de carrera administrativa, libre nombramiento, provisionales, así como los contratistas, y que desarrollan su labor dentro o fuera de las instalaciones de la UAERMV.
    - Ciudadanía en General: Cualquier ciudadano habitante del Distrito Capital que desee obtener cualquier tipo de información pública referente a la seguridad y privacidad de la información.
    - Actores Políticos o entes externos: concejales, ediles, representantes políticos de la ciudadanía con poder de decisión, así como las demás entidades con funciones de vigilancia y control de gestión de las entidades públicas.
    - Mensaje y medios de comunicación: Los mensajes a transmitir se adecuarán a los distintos grupos que forman la audiencia, mediante comunicaciones escritas, página web, reuniones, carteleras internas, Intranet, Audios y correos institucionales, Redes sociales, correos internos, audios, carteleras y anuncios en vivo por medio del sistema de sonido, Vocerías institucionales, plataformas digitales de la entidad.

## **METODOLOGIA.**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, adopta el ciclo de vida PHVA, que, a través de la mejora continua, se gestiona en su totalidad el Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

## **Ilustración 8. Metodología PHVA.**



**Fuente: Desarrollo Propio.**

* **Planear:** En esta etapa se deben cumplir las siguientes acciones:

* Determinarel alcance del sistema en términos del negocio, la entidad, su localización, activos y tecnologías.
* Fijar una política de seguridad.
* Identificar, analizar y evaluar los riesgos.
* Evaluar alternativas de tratamiento de riesgos para aplicar controles adecuados.
* Definir una declaración de aplicabilidad que incluya los objetivos de los controles mencionados.
* **Hacer.** En esta fase, se realiza la implementación del Sistema de Gestión de Seguridad de la Información. Para lo cual, se deben tomar decisiones como:
  + Establecer e implantar un plan de tratamiento de riesgos.
  + Implementar los controles anteriormente seleccionados.
  + Definir un sistema de métricas para medir la eficacia de los controles.
  + Implantar procedimientos para detectar y resolver los incidentes de seguridad.
* **Verificar.** Abarca las tareas para la monitorización, las cuales son:
  + Revisar regularmente la efectividad del sistema.
  + Medir la efectividad de los controles planteados.
  + Actualizar los planes de seguridad.
  + Revisar las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables.
* **Actuar.** Las acciones que se desarrollan en esta fase deben darse regularmente:
  + Instaurar las mejoras a identificar en el Sistema de Gestión de Seguridad de la Información.
  + Comunicar las mejoras a todas las partes interesadas con detalles y precisión.
  + Garantizar que las mejoras implantadas logren los objetivos previstos.

## **RECURSOS**

El origen de los recursos que harán parte para alcanzar las metas dentro de cada una de las fases del plan de seguridad y privacidad de la información, provienen del proyecto de inversión de Fortalecimiento de los componentes de TI para la transformación digital, y a su vez se articula con el modelo de gestión de Tecnologías de la Información definido en el actual Plan Estratégico de Tecnologías de la Información, donde se determina la necesidad de contar con herramientas tecnológicas de seguridad como: talento humano capacitado, procesos estandarizados, herramientas para la prevención de fuga de información, sistemas de prevención y detección de intrusos, herramientas de análisis de vulnerabilidades, correlacionador de eventos, herramientas para la protección de aplicaciones web, entre otros, que de manera articulada detecten oportunamente riesgos, amenazas, eventos e incidentes.

## **MAPA DE RUTA.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **ACTIVIDAD** | **FECHA FINAL** | **RESPONSABLE** | **PRODUCTO** |
| **1. ACTIVOS DE INFORMACION** | | | | |
| **1.1** | **Actualización instrumentos de identificación de activos de información** | ene-21 | OAP-GDOC | Instrumentos de Identificación de Activos |
| **1.2** | **Actualización de Activos de información** | abr-21 | Todos los Procesos | Matriz de Activos de Información |
| **1.3** | **Publicación Instrumentos de activos de información** | jun-21 | OAP | Matriz de Activos publicada en portal WEB. |
| **1.4** | **Registros activos de información ley 1712** | jun-21 | OAP | Matriz de Activos de Información |
| **1.5** | **Reporte Datos Personales** | dic-21 | Especialista Seguridad de la Información | Reporte de Bases de datos reportadas RNBD. |
| **2. RIESGOS DE ACTIVOS DE INFORMACIÓN.** | | | | |
| **2.1** | **Identificación y Análisis de Riesgos Seguridad de la información** | may-21 | Todos los Procesos | Matriz de Riesgos procesos |
| **2.2** | **Publicación de riesgos de seguridad de información** | jun-21 | OAP | Matriz de riesgos en Transparencia |
| **2.3** | **Tratamiento de Riesgos Seguridad de la Información** | dic-21 | Todos los Procesos | Matriz de riesgos procesos, Actas de Reunión, Correos |
| **2.4** | **Información de seguridad Seguimiento de Riesgos y Revisión-Informe** | dic-21 | OCI | Informe de Riesgos |
| **3. PLAN DE CONCIENCIACIÓN SEGURIDAD DE LA INFORMACIÓN.** | | | | |
| **3.1** | **Elaboración Plan de concienciación.** | dic-21 | Especialista Seguridad de la Información | Documento Plan de Concienciación en Seguridad y Privacidad |
| **3.2** | **Ejecución Plan de Concienciación.** | dic-21 | Especialista Seguridad de la Información | Informe de ejecución |
| **3.3** | **Análisis de Resultados Plan de Concienciación.** | dic-21 | Especialista Seguridad de la Información | Informe de resultados Plan de Concienciación en Seguridad y Privacidad |
| **6. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.** | | | | |
| **4.1** | **Atención de Incidentes de Seguridad de la Información** | dic-21 | Especialista Seguridad de la Información | Formato atención de incidentes. |
| **4.2** | **Divulgar boletines informativos de seguridad, Integrar con CSIRT de Gobierno** | dic-21 | Especialista Seguridad de la Información | Correo de alertas de seguridad y/o recomendaciones. |

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por:** | **Validado por**  **Líderes (Estratégico u Operativo) del Proceso:** | **Aprobado:** |
| **LUIS ENRIQUE PARIS GARCIA /**  **GLORIA MENDEZ**  **Contratista / Proceso EGTI** | Firma: | Firma: |
| **Acompañamiento Asesor OAP:** |
| **ANDREA DEL PILAR ZAMBRANO BARRIOS**  **Contratistas/ Proceso DESI** |
| **LUZ DARY CASTAÑEDA HERNANDEZ**  **Secretaria General (E)** | **CLARA INÉS SALCEDO ROJAS**  **Representante de la Alta Dirección (E)** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección** |
| 1 | Elaborada por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), versión inicial del documento conforme a los requerimientos de MINTIC. | Febrero 2019 | Jefe Oficina Asesora de Planeación |
| 2 | Se modifica la codificación del documento para adecuarlo a la estructura de documental de la nueva plataforma estratégica y debido a que el código EGTI-PL-001 se asignó en primera instancia al Plan Estratégico de Tecnologías de la Información PETI. | Mayo  2019 | Jefe Oficina Asesora de Planeación |
| 3 | Se actualiza el plan para presentar los temas y actividades que contempla desarrollar la UMV en su Plan de Seguridad y Privacidad de la información. | Enero  2020 | Jefe Oficina Asesora de Planeación |
| 4 | Se reestructura documento, se modifica introducción, se modifican objetivos generales y específicos, articulándolos con el MSPI, se alinea a lo establecido con la NIST 800-53. | Diciembre 2020. | Jefe Oficina Asesora de Planeación |