

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

**Bogotá, D.C.,**

**DICIEMBRE DE 2021**

**Contenido**

[**1.** **INTRODUCCION** 4](#_Toc89099199)

[**2.** **OBJETIVOS** 5](#_Toc89099200)

[**2.1.** **General** 5](#_Toc89099201)

[**2.2.** **Específicos** 5](#_Toc89099202)

[**3.** **ALCANCE** 5](#_Toc89099203)

[**4.** **GLOSARIO** 6](#_Toc89099204)

[**4.1.** **SIGLAS** 7](#_Toc89099205)

[**5.** **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** 7](#_Toc89099206)

[**6.** **METODOLOGIA.** 8](#_Toc89099207)

[**6.1.** **Ciclo De Operación** 8](#_Toc89099209)

[**6.2.** **Ciclo de funcionamiento del modelo de operación (PHVA).** 9](#_Toc89099211)

[**6.3.** **Alineación Norma ISO 27001:2013 vs Ciclo de Operación.** 9](#_Toc89099212)

[**7.** **CONTEXTO INSTITUCIONAL.** 10](#_Toc89099214)

[**7.1.** **Misión.** 10](#_Toc89099215)

[**7.2.** **Visión** 10](#_Toc89099216)

[**8.** **ALINEACIÓN DE LA ESTRATEGIA DE TI CON LA ESTRATEGIA DE LA UAERMV** 10](#_Toc89099217)

[**Tabla No. 1. Relación entre los Objetivos Institucionales y la Estrategia de TI.** 11](#_Toc89099219)

[**8.1.** **Análisis de Entornos** 12](#_Toc89099220)

[**8.1.1.** **Análisis Externo.** 12](#_Toc89099221)

[**8.1.2.** **Análisis Interno.** 13](#_Toc89099223)

[**9.** **SITUACIÓN ACTUAL** 14](#_Toc89099224)

[**9.1.** **Diagnóstico Seguridad de la Información – Instrumento MinTIC.** 14](#_Toc89099225)

[**10.** **ANALISIS Y PRIORIZACIÓN DE INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN.** 14](#_Toc89099226)

[**11.** **RECURSOS** 17](#_Toc89099229)

[**12.** **MAPA DE RUTA.** 18](#_Toc89099230)

**TABLAS E ILUSTRACIONES**

[**Ilustración No. 1. Metodología de Operación.** 8](#_Toc89099208)

[**Ilustración No. 2. Ciclo de Operación.** 9](#_Toc89099210)

[**Ilustración No. 3. Alineación norma ISO 27001:2013 al Ciclo Mejora Continua.** 10](#_Toc89099213)

[**Ilustración No. 4. Objetivos Institucionales y Objetivos de TI** 11](#_Toc89099218)

[**Ilustración No. 5. PESTAL.** 12](#_Toc89099222)

[**Tabla No. 2. Necesidades Seguridad de la Información.** 15](#_Toc89099227)

[**Tabla No. 3. Requerimientos Seguridad de la Información.** 16](#_Toc89099228)

# **INTRODUCCION**

El presente documento describe el Plan de Seguridad de la Información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, el cual se encuentra alineado con los objetivos y metas institucionales.

Por consiguiente, y siguiendo las pautas dadas por el Ministerio de Tecnología de la Información y Comunicaciones - MinTIC, a través del Modelo de Seguridad y Privacidad de la Información - MSPI, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, incorpora las acciones correspondientes en materia de seguridad en pro de la protección de los activos de información de la entidad, permitiendo a través de la adopción de controles la mitigación de riesgos asociados a los activos de información.

Adicional, en el presente documento se plantean una serie de iniciativas que tienen como finalidad el fortalecimiento y mejoramiento de la seguridad de la información al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, permitiendo hacer frente a las posibles amenazas a las cuales se encuentra expuesta, mitigando posibles incidentes de seguridad de la información.

Finalmente, el documento plantea un mapa de ruta que sirve como base para el fortalecimiento y mejoramiento de seguridad de la información en cada uno de los procesos y/o áreas de la entidad.

# **OBJETIVOS**

# **General**

Establecer las actividades necesarias para la generación e implementación de políticas, controles, lineamientos, procedimientos y buenas prácticas que contribuyan con la preservación de la confidencialidad, integridad y disponibilidad de los activos tecnológicos de la entidad.

# **Específicos**

* Avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información, mejorando el nivel de madurez de la entidad en materia de seguridad.
* Fortalecer el uso y apropiación en materia de seguridad digital al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.
* 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.
* Definir políticas y controles que contribuyan con la seguridad de la información de la entidad.
* Apoyar e impulsar la innovación tecnológica en la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

## **ALCANCE**

El presente documento define la hoja de ruta de las iniciativas que se deben seguir para las siguientes vigencias con el propósito de adelantar las acciones y planes de trabajo que permitan ejecutar la política de seguridad de la información de la entidad junto con el avance de la implementación del Modelo de Seguridad y Privacidad de la información contribuyendo con la protección de los activos tecnológicos al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

## **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.
* **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 información.
* **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.
* **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.
* **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.

## **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 el Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

## **Ilustración No. 1. Metodología de Operación.**

Diagrama

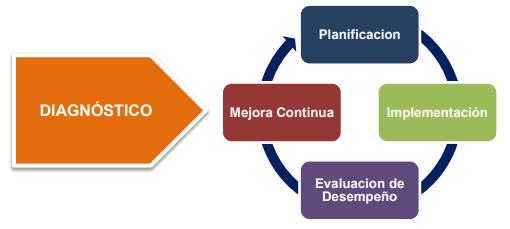
Descripción generada automáticamente

**Fuente:** Desarrollo Propio.

## **Ciclo De Operación**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, desarrolla 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 como se mencionan a continuación:

## **Ilustración No. 2. Ciclo de Operación.**



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

La ilustración 2 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.

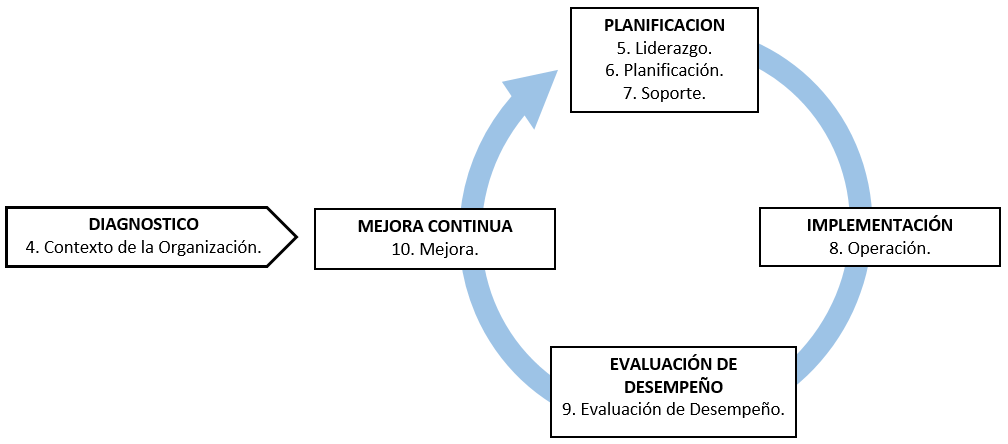
## **Ciclo de funcionamiento del modelo de operación (PHVA).**

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 evaluación MSPI, se logra determinar el nivel de cumplimiento del ciclo definido dentro del Modelo de Seguridad y Privacidad de la Información.

## **Alineación 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 No. 3. Alineación norma ISO 27001:2013 al Ciclo Mejora Continua.**



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

# **CONTEXTO INSTITUCIONAL.**

# **Misión.**

Somos una entidad técnica descentralizada y adscrita al sector movilidad de Bogotá D.C, encargada de conservar la malla vial local, intermedia y rural, así como la ciclo-infraestructura y de atender situaciones imprevistas que dificultan la movilidad. Además, brindamos apoyo interinstitucional y realizamos obras complementarias para la mejora de la seguridad vial y la adecuación del espacio público peatonal cuando sea requerido, con el fin de mejorar la calidad de vida de los ciudadanos.

# **Visión**

En el 2030 seremos una entidad reconocida por su gestión eficiente para el mejoramiento del subsistema vial, con total autonomía presupuestal y referente nacional e internacional por el desarrollo de un modelo sostenible de conservación que genera valor público y facilita la conectividad multimodal para el uso y disfrute de los habitantes de la ciudad-región.

## **ALINEACIÓN DE LA ESTRATEGIA DE TI CON LA ESTRATEGIA DE LA UAERMV**

En la siguiente ilustración se puede visualizar la relación entre los objetivos institucionales de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial y los objetivos de TI. Los objetivos de TI viabilizan el cumplimiento de los objetivos misionales, estratégicos y de apoyo de la entidad. Posteriormente se describen las estrategias de TI que soportan los objetivos del negocio.

# **Ilustración No. 4. Objetivos Institucionales y Objetivos de TI**



**Fuente:** Proyecto GODI

# **Tabla No. 1. Relación entre los Objetivos Institucionales y la Estrategia de TI.**

| **Objetivo Institucional de la UAERMV** | **Estrategia de TI** |
| --- | --- |
| Liderar la política pública de la conservación de la infraestructura vial local de Bogotá D.C. | Automatización de los procesos misionales, gobierno de información, generación de diversas capacidades organizacionales (tales como inteligencia de negocios, arquitectura empresarial e interoperabilidad) y apropiación tecnológica para apoyar la política pública de la conservación de la infraestructura vial que sea adoptada por la entidad. |
| Mejorar las condiciones de movilidad de la malla vial, a través de los programas de conservación y la atención de situaciones imprevistas que dificulten la movilidad en Bogotá D.C | Fortalecimiento de los sistemas de información y gobierno de la información, captura de información en terreno a través de dispositivos móviles, servicios tecnológicos, seguridad de la información, soporte tecnológico; en aras de ofrecer las condiciones tecnológicas necesarias para soportar la gestión de los programas de conservación que la entidad aplique, así como apoyar estratégicamente el diseño de estos. |
| Optimizar la infraestructura técnica, tecnológica y organizacional de la entidad para el cumplimiento de su nacionalidad. | Disponibilidad de la infraestructura tecnológica adecuada para soportar las necesidades de la entidad, en condiciones de seguridad y con una gestión de servicios de calidad y oportuna. |
| Mejorar la gestión institucional a través de mecanismos de transparencia y eficiencia de los procesos para la toma de decisiones y la mejora continua en pro de la satisfacción del ciudadano y grupos de valor. | Fortalecimiento de la seguridad y privacidad de la información, soporte de procesos mediante sistemas de información y aplicación de un gobierno de información con el ánimo de disponer de información de calidad y oportuna para facilitar la toma de decisiones. |
| Desarrollar una cultura organizacional fundamentada en el fortalecimiento del talento humano a través de la gestión del conocimiento, su apropiación y aprovechamiento y la mejora del clima laboral, como motores de la generación de resultados de la entidad. | Empoderamiento del grupo de TI para adoptar capacidades que permitan incrementar la madurez tecnológica de la entidad y fortalecimiento del uso y apropiación tecnológica dentro de la UAERMV en aras de alinear el desarrollo de la entidad con las capacidades de su talento humano. |

**Fuente:** Proyecto GODI

# **Análisis de Entornos**

Este apartado consiste en identificar los aspectos externos e internos relevantes para la entidad; este ejercicio aporta en la construcción de la perspectiva sistémica de la Planeación Estratégica.

Para la caracterización del entorno externo, se ha acudido al modelo PESTAL que es una herramienta tradicional en el Direccionamiento Estratégico, en el cual se analizan seis dimensiones: política, económica, social, tecnológica, ambiental y legal relacionadas con la entidad. Así mismo, para el análisis del entorno interno se propuesto la identificación de la metodología DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas) que es la identificación de las variables positivas, negativas, internas y externas a nivel de TI.

# **Análisis Externo.**

## **Ilustración No. 5. PESTAL.**

Diagrama, Escala de tiempo

Descripción generada automáticamente

**Fuente:** Desarrollo Propio.

# **Análisis Interno.**

* Icono

  Descripción generada automáticamente con confianza mediaLas adquisiciones, iniciativas y proyectos de TI consignadas en el PETI están sujetas al presupuesto asignado para el proyecto de inversión relacionado.
* El mejoramiento en la gestión de la capacidad y disponibilidad están basados en parte, en la adquisición de elementos tecnológicos que dependen del presupuesto disponible.
* Grupo de TI no cuenta con un representante técnico dentro del comité directivo por lo que se pierden oportunidades estratégicas de fortalecer las acciones dispuestas por la alta gerencia de la UAERMV.
* Riesgo de pérdida de información debido a que no están apropiadas dentro de la entidad las políticas referentes a la seguridad de la información.
* Interfaz de usuario gráfica, Aplicación

  Descripción generada automáticamenteAl disponer de una planeación estratégica de tecnologías de la información (PETI) se estructuran las diferentes acciones desde tecnología para soportar la operación de la UAERMV y alcanzar sus objetivos institucionales.
* La existencia de tecnologias emergentes pueden llegar a soportar eficientemente los flujos de negocio.
* Teniendo en cuenta la contingencia por la pandeminia los sistemas de información y herramientas de TI son adoptados por la entidad de forma permanente.
* La existencia de buenas prácticas en los diferentes dominios de la Arquitectura Empresarial permite optimizar la gestión de las diferentes actividades del grupo de TI.
* Icono

  Descripción generada automáticamenteLa definición de un nuevo proceso de Estrategia y Gobierno de TI permite diferenciar las actividades estratégicas desarrolladas por el grupo de TI para la generación de herramientas y sistemas de información, logrando dar mayor agilidad a las operaciones de los procesos misionales.
* El grupo de TI ofrece estrategias y soluciones a las diferentes dependencias de la UAERMV que permiten optimizar sus procesos en aras de alcanzar los objetivos institucionales.
* La aplicación de la soluciones ofrecidas por el proceso permite fortalecer el empoderamiento del grupo de tecnología en el manejo de proyectos institucionales con componente de TI.
* Teniendo en cuenta la contingencia por la pandeminia la entidad contaba con la herramientas tecnologicas y sistemas de información que hizo posible el trabajo en casa sin causar traumatismos ni indisponibilidad de los servicios.

Icono

Descripción generada automáticamente

* La gestión de activos esta alineada con la política de seguridad, lo que genera la necesidad de adquisición de elementos tecnológicos que a su vez dependen del presupuesto disponible.
* La no ejecución del presente documento por parte de la nueva administración obstaculiza la continuidad de las acciones planteadas para alcanzar la visión de la UAERMV.
* Los cambios permanentes en la tecnología y normatividad.

# **SITUACIÓN ACTUAL**

Describe la línea base a noviembre 2021 del estado del Modelo de Seguridad y Privacidad de la Información al interior de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, a través del instrumento de diagnóstico emitido por el Ministerio de Tecnologías de Comunicaciones de Colombia- MinTIC, el cual permite establecer el nivel de madurez con respecto a seguridad de la información.

# **Diagnóstico Seguridad de la Información – Instrumento MinTIC.**

A partir del autodiagnóstico adelantado en la vigencia 2021 se evidencia el avance y mejoramiento en el nivel de madurez alcanzado por la entidad para cada uno de los dominios en seguridad de la información, definidos en el modelo de seguridad.

Este nivel de madurez se determina con los resultados obtenidos en la herramienta de diagnóstico de seguridad y privacidad de la información provista por el Ministerio de Tecnologías de Comunicaciones de Colombia - MinTIC, el cual a su vez permite establecer las bases para la mejora continua en materia de Seguridad de   
la Información e identificar las iniciativas correspondientes en seguridad de la información, los cuales deben estar alineadas a las necesidades identificadas en Plan Estratégico de Tecnologías de Información y Comunicaciones (PETI).

# **ANALISIS Y PRIORIZACIÓN DE INICIATIVAS DE SEGURIDAD DE LA INFORMACIÓN.**

Teniendo en cuenta los resultados del autodiagnóstico, se identifican iniciativas de seguridad de la información, las cuales permitirán el fortalecimiento y mejoramiento de la seguridad de la información de manera interna como externa de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial. En virtud de lo anterior, se identifican las siguientes necesidades y requerimientos correspondientes:

## **Tabla No. 2. Necesidades Seguridad de la Información.**

| **ID** | **NECESIDAD** | **DESCRIPCIÓN** |
| --- | --- | --- |
| **SG-NC-PEH** | Pruebas Ethical Hacking | Con el objetivo de fortalecer la infraestructura tecnológica de la entidad se necesita realizar pruebas de penetración e Intrusión, permitiendo la identificación y corrección temprana de las brechas de seguridad minimizando posibles eventos o incidentes de seguridad. |
| **SG-NC-PLS** | Plan de Sensibilización | Con el objetivo de fortalecer y crear conciencia en seguridad de la información en cada una de las personas que brindan sus servicios en pro de la entidad, se hace necesario el contar con Capacitaciones correspondientes en seguridad de la información que fomenten las buenas prácticas al interior. |
| **SG-NC-PFI** | Prevención de Fuga DLP | Con el objetivo de proteger la información sensible de la entidad contra fuga de información, se hace necesario contar con soluciones y/o herramientas que monitoricen la red de la entidad. |
| **SG-NC-BYOB** | Bring Your Own Device | Con el objetivo de proteger la información y el acceso a la red corporativa, se hace necesario contar con herramientas y/o soluciones que controlen y monitoricen todos los dispositivos externos que intenten conectarse a la red institucional. |
| **SG-NC-SGD** | Cambio Sistema de Información Gestión Documental | Con el objetivo de mitigar las brechas de seguridad con las que cuenta el gestor documental y en pro del aumento de las capacidades de conservación y preservación digital, se hace necesario contar con un nuevo sistema de gestión documental que cuente con soporte y con los niveles de seguridad adecuados. |
| **SG-NC-VID** | Virtualización | Con el objetivo de minimizar los riesgos asociados a la pérdida de información, fuga de información, obsolescencia tecnológica, se hace necesario contar con esquemas de virtualización que permitan la interacción de forma adecuada con la infraestructura tecnológica de la entidad |
| **SG-NC-AKY** | AntiKeyLogger | Con el objetivo de proteger la integridad de información financiera y en cumplimiento de la resolución SDH-316, se hace necesario contar con herramientas tecnológicas que impidan la captura de la digitación de teclas por parte de las personas que desempeñan esta labor. |
| **SG-NC-AMW** | Antimalware | Con el objetivo de proteger a la red corporativa de posible infección de software malicioso, se hace necesario contar con herramientas y/o soluciones que analicen el tráfico de información de la red, permitiendo la detección y contención de posibles softwares maliciosos. |
| **SG-NC-DDOS** | AntiDDOS | Con el objetivo de proteger la disponibilidad de los servicios de la entidad, se hace necesario contar con herramientas y/o soluciones que permitan prevenir ataques de denegación de servicio. |
| **SG-NC-IPS** | IDS - IPS | Con el objetivo de prevenir posibles eventos y/o incidentes de seguridad de la información, se hace necesario contar con herramientas y/o soluciones que permitan monitorear de forma activa la infraestructura tecnológica de la entidad. |
| **SG-NC-MBS** | Membresías | Con el objetivo de conocer de forma temprana vulnerabilidades y buenas prácticas en la materia, se hace necesario contar con membresías a comunidades que permitan conocer alertas tempranas que minimicen posibles eventos y/o incidentes de seguridad. |

**Fuente:** Desarrollo Propio.

## **Tabla No. 3. Requerimientos Seguridad de la Información.**

| **ID** | **REQUERIMIENTO** | **DESCRIPCIÓN** |
| --- | --- | --- |
| **SG-RQ-GVT** | Gestión de Vulnerabilidades | Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. |
| **SG-RQ-DRP** | Plan Recuperación de Desastres | Asegurar la disponibilidad de instalaciones de procesamiento de información.  Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. |
| **SG-RQ-BCP** | Plan Continuidad de Negocio | La entidad debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. Esta actividad deberá ser gestionada por la Oficia Asesora de Planeación. |
| **SG-RQ-MSPI** | Revisión Independiente Seguridad de la Información | Esta revisión la deberían llevar a cabo individuos independientes del área que se revisa, por ejemplo, la función de auditoría interna, un gerente independiente o una parte externa de la organización que se especializa en estas revisiones. Los individuos que llevan a cabo estas revisiones deberían contar con las habilidades y experiencia apropiadas. |
| **SG-RQ-GSC** | Gestor de Contraseñas | Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. |
| **SG-RQ-SBS** | Borrado Seguro | Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software licenciado haya sido  retirado o sobrescrito en forma segura antes de su disposición o reúso. |

**Fuente:** Desarrollo Propio.

## **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.**

El mapa de ruta planteado, brinda la posibilidad de visualizar y organizar las estrategias y actividades consecuentes a los siguientes pasos a ejecutar. Este mapa de ruta será gestionado por la Oficina Asesora de Planeación quien será la encargada de tramitar de forma transversal el levantamiento de los activos de información por cada uno de los procesos de la entidad:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **ACTIVIDAD** | **FECHA FINAL** | **RESPONSABLE** | **PRODUCTO** |
| **1. ACTIVOS DE INFORMACION** | | | | |
| **1.1** | **Actualización instrumentos de identificación de activos de información** | Feb-22 | OAP-GDOC | Instrumentos de Identificación/ actualización de Activos de información |
| **1.2** | **Actualización de Activos de información** | Ago-22 | Todos los Procesos | Matriz de Activos de Información |
| **1.3** | **Publicación Instrumentos de activos de información** | Oct-22 | OAP | Matriz de Activos publicada en portal WEB. |
| **1.4** | **Registros activos de información ley 1712** | Sep-22 | 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** | Sep-22 | Todos los Procesos | Matriz de Riesgos procesos |
| **2.2** | **Publicación de riesgos de seguridad de información** | Oct-22 | OAP | Matriz de riesgos en Transparencia |
| **2.3** | **Tratamiento de Riesgos Seguridad de la Información** | dic-22 | Todos los Procesos | Matriz de riesgos procesos, Actas de Reunión, Correos |
| **2.4** | **Información de seguridad Seguimiento de Riesgos y Revisión-Informe** | dic-22 | OCI | Informe de Riesgos |
| **3. PLAN DE CONCIENCIACIÓN SEGURIDAD DE LA INFORMACIÓN.** | | | | |
| **3.1** | **Elaboración Plan de concienciación.** | ago-22 | 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. |

|  |  |  |
| --- | --- | --- |
| **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:** |
| **CHRISTIAN MEDINA FANDIÑO**  **Contratistas/ Proceso DESI** |
| **MARTHA PATRICIA AGUILAR COPETE**  **(Secretaria General)** | **JUAN HERNANDO LIZARAZO**  **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 |
| 5 | Se ajustan objetivos específicos, se incorporan necesidades y requerimientos de seguridad de la información. | Diciembre 2021. | Jefe Oficina Asesora de Planeación |