# SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMAION SGSI – GOBERNACION DEL CESAR - 2022

| Detalle del Documento | |
|---|---|
| Nombre de Documento | Plan de seguridad y privacidad de la Información |
| Versión del Documento | 1.4 |
| Fecha | 30/11/2022 |
| Detalle | Este habilitador busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad, y privacidad de la información (MinTIC). |

| Control de Cambios | | |
|---|---|---|
| **Fecha** | **Versión** | **Descripción** |
| 10/12/2021 | 1.2 | Seguimiento |
| 10/12/2021 | 1.3 | Actualización y seguimiento |
| 30/11/2022 | 1.4 | Actualización y seguimiento |
| | | |

| Control de Aprobación | | | |
|---|---|---|---|
| **Variables** | **Fecha** | **Nombre** | **Cargo o Perfil** |
| Elaboró | 21/11/2022 | Hugo Alberto Puche Espinosa | Profesional Especializado |
| Revisó | 30/11/2022 | Miguel Ángel Aroca Cervantes | Asesor TIC |
| Aprobó | 10/12/2022 | Comité de Gestión y Desempeño | |

# Tabla de contenido

# 1. GENERALIDADES – CONOCIMIENTO DE LA ENTIDAD

## 1.1 Introducción.

La política del gobierno nacional en el marco del Decreto 1078 del 2015 “Decreto único reglamentario del sector TIC” y en cumplimiento del decreto 767 de 2022, establece los lineamientos generales de la Política de Gobierno Digital, entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos en todo el territorio nacional y mejorar la competitividad del país, mediante la generación de valor público a través de la transformación digital del Estado, de una manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés, que permita el ejercicio de los derechos de los usuarios del ciberespacio.

El gobierno nacional a través del Plan Nacional de Desarrollo 2018 – 2022 “Pacto por Colombia pacto por la Equidad”, establece la importancia de las tecnologías de la información y comunicaciones como fuente y pilar para el desarrollo de las regiones de Colombia, para ello, el Plan TIC 2019 – 2022 “El futuro digital es de todos”, establece cuales son las directrices y lineamientos que las entidades públicas deben tener en cuenta para el desarrollo y fortalecimiento institucional de las TIC.

Los habilitadores transversales de la política de Gobierno Digital: Arquitectura, Seguridad y privacidad de la Información, cultura y apropiación, y Servicios Ciudadanos Digitales; son elementos fundamentales que permiten el despliegue de los componentes de la política y tienen como objetivo, desarrollar capacidades en cada entidad para la implementación de la política.

Específicamente el habilitador de seguridad y privacidad de la información, está definido de la siguiente manera:

> “**Seguridad y Privacidad de la Información:** Este habilitador busca que las entidades públicas desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.”

El Departamento del Cesar, en cumplimiento a las Políticas y Directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) a través del Decreto 612 del 4 de abril de 2018 y Decreto 1078 de 2015, implementará actividades de planeación estratégica para el control y administración efectiva de los riesgos y las necesidades de seguridad de la información de la entidad.

Una vez socializado el presente plan, los funcionarios, contratistas y terceros de la entidad adoptarán los controles de seguridad y privacidad de la información en sus procesos, con el fin de minimizar los riesgos que puedan afectar la seguridad y privacidad de la información.

## 1.2 Objetivo general

Implementar estrategias que permitan garantizar la seguridad y privacidad de la información para cada uno de sus pilares (Integridad, Disponibilidad y Confidencialidad), en la Gobernación del Departamento del Cesar.

## 1.3 Objetivos específicos

- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de planificación.
- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de implementación.
- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de evaluación y desempeño.
- Realizar a través de las actividades de cada una de las metas, los resultados de la fase de mejora continua.

## 1.4 Alcance

El presente plan aplica a todos los procesos de la entidad, a los líderes de cada proceso, a los funcionarios definidos con el rol de custodio y propietario de la información, a terceros que en razón del cumplimiento de sus obligaciones contractuales con el Departamento del Cesar compartan, utilicen, recolecten, procesen, intercambien o consulten su información, a los entes de control y entidades relacionadas que accedan, ya sea desde la red interna o externa a cualquier activo de información. Así mismo, este plan aplica a toda la información creada, procesada o utilizada por la entidad, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

## 1.5 Marco normativo

- Constitución Política de Colombia. Artículo 15.
- Constitución Política de Colombia. Artículos 209 y 269.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 767 del 2022. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario.
- Resolución 500 de 2021, MinTIC. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.

## 1.6 Documentos de Referencia

- Norma ISO/IEC 27001:2013.
- Modelo de Seguridad y Privacidad de la Información de Gobierno Digital –MSPI.
- Instrumento de Evaluación MSPI (MINTIC).

## 1.7 Definiciones

**ACTIVO**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

**ALCANCE**: ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información.

**AMENAZA:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

**ANÁLISIS DE RIESGOS**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

**ANÁLISIS DE RIESGOS CUALITATIVO**: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

**CONFIDENCIALIDAD**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**CONTROL**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**CONTROL CORRECTIVO**: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

**CONTROL DETECTIVO:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

**CONTROL DISUASORIO**: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

**CONTROL PREVENTIVO**: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

**ESTIMACIÓN DE RIESGOS**: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

**EVALUACIÓN DE RIESGOS**: Proceso global de identificación, análisis y estimación de riesgos.

**FASE DIAGNOSTICO**: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

**FASE EVALUACIÓN DE DESEMPEÑO (V**ERIFICAR**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

**FASE IMPLEMENTACIÓN (H**ACER**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

**FASE PLANIFICACIÓN (P**LANEAR**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

**FASE MEJORA CONTINUA (A**CTUAR**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

**GESTIÓN DE RIESGOS**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

**INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**INVENTARIO DE ACTIVOS**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

**INTEGRIDAD**: Propiedad de la información relativa a su exactitud y completitud.

**ISO/IEC 27001:2013**: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

**MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI):** El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

**RIESGO**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

**RIESGO RESIDUAL**: El riesgo que permanece tras el tratamiento del riesgo.

**SELECCIÓN DE CONTROLES:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

**SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**: Un sistema de Gestión para la seguridad de la información consta de una serie de políticas, procedimientos e instrucciones o directrices específicas, para cada actividad o sistema de información, que persiguen como objetivo la protección de los activos de información en una organización.

## 2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Gobernación del Departamento del Cesar en el proceso de creación del plan de seguridad de la información, se basó en el modelo PHVA que se encuentra en la guía “Plan de seguridad de la información”, de la versión 1 del modelo de gestión TI propuesto por el MinTIC.

Este modelo consta de cuatro fases y una fase previa a la implementación

| Modelo PHVA aplicado al MSPI | |
|---|---|
| **PLANIFICAR (establecer el MSPI)** | Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización. |
| **HACER (implementar y operar el MSPI)** | Implementar y operar la política, los controles, procesos y procedimientos del MSPI |
| **VERIFICAR (hacer seguimiento y revisar el MSPI)** | Evaluar y, en donde sea aplicable, medir el desempeño del proceso versus la política y los objetivos de seguridad. Reportar los resultados a la dirección, para su revisión. |

| | |
|---|---|
| **ACTUAR (mantener y mejorar el MSPI)** | Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI. |

**(Fuente: Guía plan de seguridad de la información – MinTIC)**

Antes de la fase de planificación se debe tener en cuenta la fase de diagnóstico, quien a su vez debe considerar el Instrumento de Evaluación del Modelo de Seguridad y privacidad de la información propuesto por el MinTIC.

## 2.1 Fase I. Diagnóstico – Etapa previa a la implementación

**SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSI**
**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**FASE I. DIAGNÓSTICO – ETAPA PREVIA A LA IMPLEMENTACIÓN**

| N° | ACTIVIDADES | RESPONSABLES | REGISTROS | FECHA INICIO | FECHA FINAL | REALIZADO |
|---|---|---|---|---|---|---|
| 1 | Fortalecer el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Herramienta de Diagnóstico MSPI – MINTIC | 01/01/2018 | 28/02/2018 | 100% |
| 2 | Mantener y Fortalecer el nivel de madurez de seguridad y privacidad de la información en la Entidad | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Herramienta de Diagnóstico MSPI – MINTIC | 01/03/2018 | 30/04/2018 | 100% |
| 3 | Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Herramienta de Diagnóstico MSPI – MINTIC | 01/05/2018 | 31/12/2018 | 100% |
| 4 | Identificar el avance de la implementación del ciclo de operación al interior de la entidad. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Herramienta de Diagnóstico MSPI – MINTIC | 01/07/2018 | 30/07/2018 | 100% |
| 5 | Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Herramienta de Diagnóstico MSPI – MINTIC Política de protección de datos personales – Decreto 00222 del 22 de Agosto de 2019 | 01/08/2018 | 30/08/2018 | 100% |
| 6 | Identificar y fortalecer el uso de buenas prácticas en ciberseguridad. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Herramienta de Diagnóstico MSPI – MINTIC | 01/08/2018 | 30/08/2018 | 100% |

## 2.2 Fase II. Planificación

| SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI<br>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN<br>FASE. II. PLANIFICACIÓN – ETAPAS PREVIAS A LA IMPLEMENTACIÓN | | | | | | |
|---|---|---|---|---|---|---|
| | CRONOGRAMA | | | | | |
| N° | ACTIVIDADES | RESPONSABLES | REGISTROS | FECHA INICIO | FECHA FINAL | REALIZADO |
| 1 | Fortalecer la Política de seguridad y privacidad de la información | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos | Documento con la política de seguridad de la información, aprobado por la alta Dirección y socializada al interior de la Entidad. | 01/02/2021 | 31/12/2021 | 100% |
| 2 | Fortalecer los Procedimientos de seguridad de la información. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos | Procedimientos, debidamente documentados, socializados y aprobados por el Comité Institucional de Gestión y Desempeño. | 01/02/2021 | 31/12/2021 | 100% |
| 3 | Roles y responsabilidades de seguridad y privacidad de la información. | Comité Institucional de Gestión y Desempeño | Acto administrativo a través del cual se crea o se modifica las funciones del comité institucional de gestión y desempeño (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad. | 01/02/2021 | 31/12/2021 | 100% |
| 4 | Fortalecimiento en la identificación del Inventario de activos de información. | Secretaría General - Comité Institucional de Gestión y Desempeño | Matriz con la identificación, valoración y clasificación de activos de información. | 04/02/2020 | 31/12/2021 | 100% |
| 5 | Fortalecer la Integración del MSPI con el Sistema de Gestión documental | Secretaría General | Documentación de Plan de Preservación Digital | 04/02/2020 | 31/12/2021 | 100% |
| 6 | Fortalecer la identificación, Valoración y tratamiento de riesgo de seguridad de información | Comité Institucional de Gestión y Desempeño | Documento con la metodología de gestión de riesgos de seguridad de información, con el análisis y evaluación de riesgos.<br><br>Documento con el plan de tratamiento de riesgos de seguridad de información, debidamente aprobado por Comité Institucional de Gestión y Desempeño | 04/02/2020 | 31/12/2021 | 100% |
| 7 | Plan de Comunicaciones | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Documento con el plan de comunicación sensibilización y capacitación para la entidad. | 04/02/2020 | 31/12/2021 | 100% |
| 8 | Plan de transición IPv4 a IPv6. Fase I. PLANEACION | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Documentación Fase I. PLANEACIÓN IPv4 a IPv6. | 01/02/2020 | 31/12/2021 | 100% |
| | Plan de transición IPv4 a IPv6. Fase I. PILOTOS DE FUNCIONAMIENTO | Líder TIC de la entidad | Documentación IPv4 a IPv6. Fase. III PRUEBAS DE FUNCIONAMIENTO | 02/02/2022 | 31/12/2022 | 0% |

## 2.3 Fase III. Implementación

| SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI<br>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN<br>FASE. III. IMPLEMENTACIÓN | | | | | | |
|---|---|---|---|---|---|---|
| | CRONOGRAMA | | | | | |
| N° | ACTIVIDADES | RESPONSABLES | REGISTROS | FECHA INICIO | FECHA FINAL | REALIZA DO |
| 1 | Formular el plan de tratamiento de riesgo de seguridad de información. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Documentar el plan de tratamiento de riesgo de seguridad de información | 02/01/2022 | 31/12/2022 | 100% |
| 2 | Implementar el plan de tratamiento de riesgo de seguridad de información. | Líder TIC de la entidad | Ejecución de la Fase I. Planificación de la gestión de riesgo de la seguridad de información. | 02/01/2022 | 31/12/2022 | 100% |
| 3 | Implementación de controles de seguridad de información | Líder TIC de la entidad. | Documento con el plan de tratamiento de riesgos donde se detallen los controles y sus objetivos. | 02/01/2022 | 31/12/2022 | 100% |
| 4 | Elaborar o Diseñar herramienta que permita medir la eficacia de los controles de seguridad de la información. | Líder TIC de la entidad. | Formato.Doc o Formato.xls | 02/01/2023 | 31/12/2023 | 0% |
| 5 | Proponer programas de formación o capacitación en materia de seguridad de información. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Registro de los funcionarios y contratistas capacitados | 02/01/2022 | 31/12/2022 | 100% |
| 6 | Gestionar los recursos del MSPI | Líder TIC de la entidad. | Recurso Humano Recurso Tecnológico. Recurso Audiovisual. Recurso Impreso (Folletos, Afiches o pendones) | 02/01/2022 | 31/12/2022 | 100% |
| 7 | Consolidar los reportes de incidentes de seguridad de información que se encuentren con un nivel de criticidad "ALTO" O "SUPERIOR" | Líder TIC de la entidad. | Formato de Registros de Reporte de incidentes de seguridad de información | 02/01/2023 | 31/12/2023 | 0% |
| 8 | Indicadores De Gestión. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Documento con la descripción de los indicadores de gestión de Seguridad y privacidad de la información. | 02/01/2023 | 31/12/2023 | 0% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9 | Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad de información | Líder TIC de la entidad. | Procedimientos, Controles o Políticas implementados | 02/01/2023 | 31/12/2023 | 0% |
| 10 | Plan de transición Pv4 a IPv6. Fase. II IMPLEMENTACION | Líder TIC de la entidad | Implementación del protocolo IPV6 de acuerdo a lo exigido por la normatividad nacional. | 02/01/2023 | 31/12/2023 | 0% |

## 2.4 Fase IV. Evaluación del desempeño

| SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI<br>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN<br>FASE. IV. EVALUACIÓN Y DESEMPEÑO | | | | | | |
|---|---|---|---|---|---|---|
| | CRONOGRAMA | | | | | |
| N° | ACTIVIDADES | RESPONSABLES | REGISTROS | FECHA INICIO | FECHA FINAL | REALIZADO |
| 1 | Seguimiento y revisión a la implementación del MSPI. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Registros de Seguimiento y revisión | 02/01/2022 | 30/06/2022 | 100% |
| 2 | Seguimiento y revisión a la implementación del MSPI. | Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos. | Registros de Seguimiento y revisión | 01/07/2022 | 31/08/2022 | 100% |
| 3 | Realizar auditorías internas del MSPI a intervalos planificados | Líder TIC de la entidad. | Registros de Seguimiento y revisión | 02/01/2023 | 31/12/2023 | 0% |
| 4 | Seguimiento y revisión a la Auditoria Interna de seguridad de información | Líder TIC de la entidad. | Registros de Seguimiento y revisión | 02/01/2023 | 31/12/2023 | 0% |
| 5 | Seguimiento y revisión al cumplimiento de la política de seguridad de la información y Controles. | Líder TIC de la entidad. | Registros de Seguimiento y revisión | 02/01/2023 | 31/12/2023 | 0% |

## 2.5 Fase V. Mejora continua

| SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SGSPI<br>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN<br>FASE. V. MEJORA CONTINUA<br>CRONOGRAMA | | | | | | |
|---|---|---|---|---|---|---|
| N° | ACTIVIDADES | RESPONSABLES | REGISTROS | FECHA INICIO | FECHA FINAL | REALIZADO |
| 1 | Mejorar uso y apropiación de la política de seguridad de la información. | Líder TIC de la entidad. | Registros de Mejora y Actualización | 02/01/2023 | 31/12/2023 | 0% |
| 2 | Mejorar los objetivos de seguridad de la información. | Líder TIC de la entidad. | Registros de Mejora y Actualización | 02/01/2023 | 31/12/2023 | 0% |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | Mejora los resultados de la auditoría interna de seguridad de información | Líder TIC de la entidad. | Registros de Mejora y Actualización | 02/01/2023 | 31/12/2023 | 0% |
| 4 | Mejorar el Uso e Implementación de los controles de seguridad de información | Líder TIC de la entidad. | Registros de Mejora y Actualización | 02/01/2023 | 31/12/2023 | 0% |
| 5 | Mejorar el resultados de los indicadores | Líder TIC de la entidad. | Registros de Mejora y Actualización | 02/01/2023 | 31/12/2023 | 0% |