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

**VERSIÓN 1.0**

**2023**

**Contenido**

Contenido

[INTRODUCCIÓN 3](#_Toc125713491)

[OBJETIVO 4](#_Toc125713492)

[OBJETIVOS ESPECÍFICOS 4](#_Toc125713493)

[ALCANCE 5](#_Toc125713494)

[MARCO NORMATIVO 6](#_Toc125713495)

[MODELO DE SEGURIDAD Y PRIVACIDAD - MSPI 7](#_Toc125713496)

[FASE PREVIA - DIAGNOSTICO DEL MSPI 8](#_Toc125713497)

[ESTADO ACTUAL 8](#_Toc125713498)

[FASE PHVA 9](#_Toc125713499)

[FASE DE PLANEACIÓN 9](#_Toc125713500)

[FASE HACER 10](#_Toc125713501)

[La Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional de gestión y desempeño. 10](#_Toc125713502)

[FASE DE VERIFICACIÓN 11](#_Toc125713503)

[FASE DE ACTUAR 11](#_Toc125713504)

[Es importante que las Entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI 11](#_Toc125713505)

[CORNOGRAMA DE TRABAJO 12](#_Toc125713506)

# INTRODUCCIÓN

# OBJETIVO

Plantear la hoja de ruta del plan de seguridad y privacidad de la información del Instituto Nacional Para Ciegos - INCI, y los elementos que lo conforman, como marco de referencia para el establecimiento, regulación de lineamientos y medidas que permitan el aseguramiento de la protección y uso adecuado de la información y activos de información que la soportan al interior de la Entidad cumpliendo la integridad, disponibilidad y confidencialidad de la información

## OBJETIVOS ESPECÍFICOS

* Comunicar e implementar la estrategia de seguridad de la información.
* Incrementar el nivel de madurez del Instituto Nacional para Ciegos frente a la gestión de la seguridad y privacidad de la información.
* Brinda los pasos para la implementación y apropiación del Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de resguardar la información.

# ALCANCE

El Plan de Seguridad y Privacidad de la información identifica e incluye las alineaciones para la gestión del ciclo (PHVA) de operación del modelo de seguridad y privacidad de la información (MSPI), el cual tiene su campo de aplicación a todos los procesos de la entidad.

# MARCO NORMATIVO

|  |  |
| --- | --- |
| Marco Normativo | Descripción |
| Política de seguridad y privacidad de la información de Función Pública – 2018. | La Política de Seguridad de la Información de (MIPG  – Administracion Publica), con respecto a la protección de los activos de que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la  Información. |
| Manual de política de seguridad y privacidad de la información de  función pública – 2018. | Compendio de políticas aplican para todos los servidores públicos y contratistas de las entidades que procesan y/o manejan información de las entidades. Política publica de Seguridad Digital. |
| Decreto 103 de 2015, | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones |
| Manual Gobierno Digital. | Para la Implementación de la Estrategia de Gobierno Digital, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno Digital. |
| 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 2573 de 2014 | Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta  parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. |
| Decreto 1377 de 2013 | Por el cual se reglamenta parcialmente la Ley 1581de  2012. |
| Decreto 2609 de 2012. | Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del  Estado". |
| Decreto 2693 de 2012 | Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones |
| Ley estatutaria 1581  de 2012, | Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República |
| Ley 1474 de 2011 | Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la  gestión pública. Disponible en Línea |
| Decreto 4632 de 2011 | Por medio del cual se reglamenta parcialmente la Ley |
| 1474 de 2011 | Se refiere a la Comisión Nacional para la Moralización y  la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. |
| Ley 1273 de 2009, | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado |

# MODELO DE SEGURIDAD Y PRIVACIDAD - MSPI

El Modelo de Seguridad y Privacidad es un lineamiento publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, este es entregado a las entidades del Estado colombiano con el fin de que su adopción permita estar acorde con las buenas prácticas de seguridad y privacidad de la información, basado en norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para una correcta gestión de la información.

# FASE PREVIA - DIAGNOSTICO DEL MSPI

Esta fase permite por medio del uso de herramientas de diagnóstico, actividades de reconocimiento y valoración de controles de seguridad de la información, identificar cual es el estado actual de la Entidad en temas de seguridad y privacidad; el resultado de este de diagnóstico permitirá establecer el nivel de madurez en cuanto a seguridad y privacidad de la información, y así definir la hoja de ruta para las actividades en las siguientes fases del modelo.

# ESTADO ACTUAL

Teniendo en cuenta la calificación de FURAG de la vigencia, el INCI se encuentra en un puntaje de 91.8 en la política 07 de seguridad digital, adicional a esto la entidad se encuentra en la actualización de políticas de Seguridad de la información, aplicación de criterios de protección de datos, ajustes a los procedimientos de seguridad, entre otros.

# FASE PHVA

Cómo punto de partida y desde el SGSI ISO 27001 conjuntamente con la actualización del MSPI (**Anexo 1 Modelo de seguridad y privacidad de la información)**, se establece la fase de planear, ejecutar, verificar y actuar para la adopción, implementación del modelo para las entidades del orden nacional, regional, distrital.

Por lo anterior el instrumento PHVA se distribuye de la siguiente forma:

# FASE DE PLANEACIÓN

De acuerdo al anexo 1 de la actualización del MSPI, hace referencia que en esta fase se debe tener documentado:

* Comprensión de la organización y su contexto
* Necesidades y expectativas de los interesados
* Definición del alcance del MSPI
* Liderazgo y compromiso
* Política de seguridad y privacidad de la información
* Roles y responsabilidades
* Identificación de activos de información e infraestructura critica
* Valoración de los riesgos de seguridad de la información
* Recursos
* Competencia, toma de decisión y comunicación

El instituto nacional para ciegos INCI, mantiene constantemente los procesos de actualización a su MSPI por lo que para la fase de planeación se cuentan los anexos:

1. Anexo1: Cuestiones Internas - externas
2. Anexo2: Necesidades y expectativas de los interesados
3. Construcción del documento maestro del MSPI donde se encuentra el alcance del sistema
4. Compromiso de la Alta dirección
5. Actualización de la política de seguridad y privacidad de la información
6. Se crea el procedimiento de calificado y etiquetado de la información como punto de partida para la identificación y valoración de los activos de la entidad

# FASE HACER

# La Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional de gestión y desempeño.

# FASE DE VERIFICACIÓN

Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

# FASE DE ACTUAR

# Es importante que las Entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI

# CORNOGRAMA DE TRABAJO