Gobernación de Norte de Santander

SECRETARÍA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

GOBERNACION DE NORTE DE SANTANDER

SECRETARIA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES

William Villamizar
GOBERNADOR DE NORTE DE SANTANDER

Avenida 5 calles 13 y 14 Palacio de Gobierno
Tel: 5956200 - 018000185783
Email: tic@nortedesantander.gov.co
www.nortedesantander.gov.co

TABLA DE CONTENIDO

Contenido

1. INTRODUCCION

La Gobernación de Norte de Santander adopta el modelo de seguridad y privacidad de la información dada por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno Digital. Liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y transparente.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Gobernación de Norte de Santander está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad, que conducirán a la preservación de la confidencialidad, integridad, 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.

Después de realizado una fase de diagnóstico a través de la herramienta de autodiagnóstico INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD diseñada y puesta al servicio de las Instituciones o Entidades, por el área de fortalecimiento de la Gestión en TI del Estado de MINTIC, este documento contiene los puntos de mejora con relación al porcentaje de avance y madurez en Seguridad y Privacidad de la Información alcanzado por la Gobernación de Norte de Santander.

Dicho documento, que será actualizado periódicamente, permite incluir y fijar criterios y una serie de actividades que seguirán asegurando y preservando la operación, mejora continua y sostenibilidad de los procesos y poder lograr alcanzar una mejor relación de porcentaje en avance y madurez dentro del ciclo PHVA determinado por la estrategia de Gobierno Digital (GD).

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital en el Mapa de Procesos de la Gobernación de Norte de Santander, que apoye el establecimiento, operación, mejora continua y sostenibilidad acorde con los requerimientos del negocio, los lineamientos del modelo de seguridad y privacidad de la estrategia de Gobierno Digital y en cumplimiento a las disposiciones legales vigentes.

2.2. OBJETIVO ESPECIFICOS

Los siguientes son los objetivos específicos del plan de seguridad de la información y de ciberseguridad para el año 2020 que apalancan el cumplimiento del objetivo general:

- ✓ Apoyar la operación, mejora continua y sostenibilidad de la Política de Seguridad y Privacidad de la Información de la Gobernación Norte de Santander, adoptada mediante Resolución 001190 DEL 02 de Dic de 2019.
- ✓ Brindar a los usuarios internos y/o externos de la Gobernación de Norte de Santander un entorno de confianza digital en el uso y aprovechamiento de las TIC para garantizar la gobernanza, derechos, satisfacción de necesidades y la prestación de trámites y servicios, seguros y con calidad.
- ✓ Fortalecer y optimizar la gestión de la seguridad de la información y ciberseguridad al interior de la Gobernación de Norte de Santander.
- ✓ Fortalecer y optimizar la gestión de eventos y vulnerabilidades que afecten la seguridad de la información y ciberseguridad de la entidad.
- ✓ Fortalecer la cultura de seguridad y Privacidad de la Información dentro de la Gobernación Norte de Santander.
- ✓ Atender las observaciones y hallazgos de las auditorías internas y externas de control y requerimientos de seguridad de información establecidos por el Gobierno Nacional.

3. ALCANCE DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos de la Gobernación Norte de Santander, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de MINTIC con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos para la entidad.

Este plan aplica a los **Macroprocesos Estratégicos** (Direccionamiento Estratégico, Gestión de calidad, Gestión de Comunicaciones y Planeación del Desarrollo), **Macroproceso de Evaluación**(Seguimiento, Control y Evaluación), **Macroprocesos Misionales** (Gestión Compras y Contratación, Gestión Talento Humano, Gestión Tecnologías, Gestión Documental, Gestión Financiera, Gestión Jurídica y Gestión Logística), **Macroprocesos de Soporte** (Apoyo de Gestión Municipal e Institucional, Gestión de Información Territorial, Atención de Trámites y Servicio al Usuario, Gestión de Desarrollo Social, Gestión del Desarrollo de Infraestructura Territorial y Gestión de Desarrollo Económico) de la Gobernación de Norte de Santander, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento

de sus funciones y las de la Gobernación compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

4. DESCRIPCION DE MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La Gobernación de Norte de Santander adopta y aplica el modelo de seguridad y privacidad de la información contemplando 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.

4.1. CICLO OPERACIÓN vs ESTRUCTURA ISO 27001:2013

El modelo de seguridad y privacidad de la Información de la Gobernación Norte de Santander se estableció teniendo en cuenta las cinco (5) fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información de MINTIC.

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

- ✓ **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 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 Implementación (H**acer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- ✓ **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 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.

A continuación, se muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001:2013

Fase	Capitulo ISO 27001:2013[2]
Diagnostico	4. Contexto de la Organización
Planificación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación
Evaluación de desempeño	9. Evaluación de desempeño
Mejora Continua	10. Mejora

Fase DIAGNOSTICO en la norma ISO 27001:2013.
En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas 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, se 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 establece 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 IMPLEMENTACION en la norma ISO 27001:2013.
En el capítulo 8 - Operación de la norma ISO 27001:2013, se 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 EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2013.
En el capítulo 9 - Evaluación del desempeño, se define 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 para el proceso de mejora del modelo de seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectivas para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

4.2. FASES I: DIAGNOSTICO

El objetivo de esta fase es Identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información
.

Figura 2 – Etapas previas a la implementación

Tabla 2. Metas, Resultados e Instrumentos de fases previas a implementación

DIAGNOSTICO			
METAS	**RESULTADOS**	**INSTRUMENTOS MSPI**	**MRAE**
Determinar el estado actual de la gestión De seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Diligenciamiento de la herramienta de identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	EVIDENCIAS
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información. Diagnostico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013. Valoración estado actual de la gestión de seguridad de la entidad	Documento actual de Plan de Seguridad y Privacidad de la Información, de acuerdo a diagnóstico según herramienta ejecutada.
Identificar el nivel de madurez de seguridad y privacidad dela información en la Entidad.	Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de Gobierno Digital de MINTIC	
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información dela entidad y definición de planes de mitigación.	

4.3. FASES II: PLANIFICACION

El objetivo de esta fase es definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI

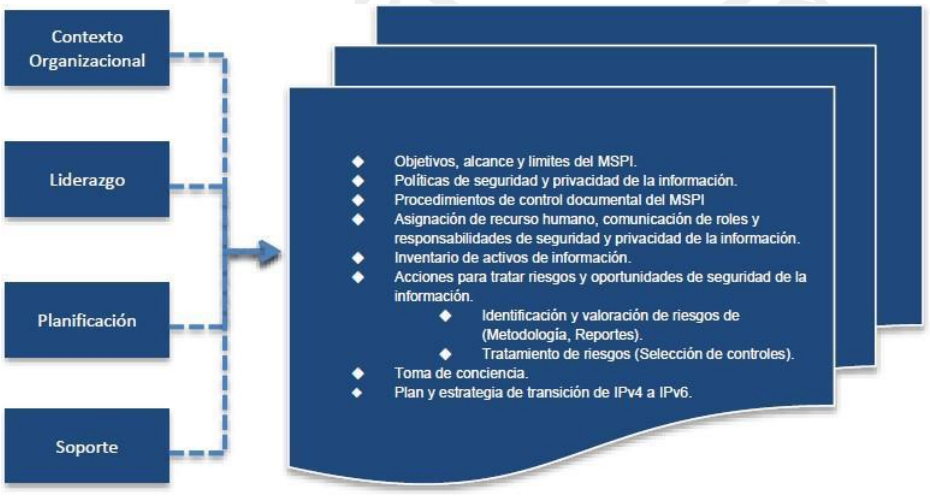

Figura 3 - Fase de planificación

Tabla 3. Metas, Resultados e Instrumentos de la de la fase de planificación

PLANIFICACION			
METAS	**RESULTADOS**	**INSTRUMENTO MSPI**	**MRAE**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía no 2 - Política General MSPI	LI.ES.09 LI.ES.10 LI.GO.01
Procedimientos de seguridad de la información	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional	Guía No 3 - Procedimientos de Seguridad y Privacidad de la	LI.GO.04 LI.GO.07
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01
Inventario de activos de información .	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información y su caracterización.	Guía No 5 - Gestión De Activos. Guía No 20 - Transición Ipv4 a Ipv6	LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01
	Inventario de activos de IPv6		LI.UA.02 LI.UA.03 LI.UA.04
Integración del MSPI con el Sistema de Gestión documento	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental	LI.UA.05

PLANIFICACION			
METAS	**RESULTADOS**	**INSTRUMENTO MSPI**	**MRAE**
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta	Guía No 7 - Gestión de Riesgos. Guía No 8 - Controles de Seguridad.	LI.UA.06
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	

SITUACION ACTUAL DE GOBERNACION N.D.S EN FASE DE PLANIFICACION

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	EVIDENCIAS
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Documento 4. Política de Seguridad y Privacidad de la Información de Gobernación de N.de.S.
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Documento Res. 001190 de 2019 Adopción de Política de Seguridad y Privacidad de
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Documento 4. Política de Seguridad y Privacidad de la Información de Gobernación N.de.S.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea el Grupo de Arquitectura Empresarial para la transformación digital de la Gobernación de N.de.S. e igualmente se definen integrantes de quienes lo conforman y sus responsabilidades, revisado y aprobado por la alta Dirección.	Documento Resol. 0010 de 27 de marzo de 2019. Grupo Trabajo de Arquitectura Empresarial de Gobernación de N.de.S..
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.	Documento 8 – Inventario de activos de Gobernación de N.de.S.

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	EVIDENCIAS
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos.	Documento 14 - Plan de Gestión de Riesgos Documento 16 - Riesgos Identificados y Valorados de acuerdo a la Metodología Documento 13 - Plan de
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Documento 6 - Plan de Sensibilización de Seguridad de la Información de la Gobernación de N.de.S.
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Documento 17. Plan de Diagnóstico y Transición de IPV4 a IPV6 IPV6 de la Gobernación de N.deS.

4.4. FASES III: IMPLEMENTACION

El objetivo de esta fase es llevar a cabo la implementación de la fase de planificación del MSPI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.

Figura 4 - Fase de implementación

Tabla 4. Metas, Resultados e Instrumentos de la de la fase de implementación

IMPLEMENTACION			
METAS	**RESULTADOS**	**INSTRUMENTO MSPI**	**MRAE**
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	LI.GO.10 LI.GO.14 LI.GO.15
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadores de Gestión SI.	LI.INF.09 LI.INF.10
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6	LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22

SITUACION ACTUAL DE GOBERNACION N.D.S EN FASE DE IMPLEMENTACION

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	EVIDENCIAS
Planificación y Control Operacional.	Documento pendiente con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. Pendiente por ejecutar durante este año pruebas vulnerabilidades e intrusión con el objetivo de identificar el nivel de protección de los activos de información de la entidad. Pendiente por ejecutar durante este año el plan anual de capacitación, socialización y sensibilización de seguridad de la información Pendiente por ejecutar durante este año pruebas de Ethical Hacking orientadas a poder determinar los niveles de riesgo y exposición de la organización ante atacantes interno o externo que puedan a comprometer activos críticos de la entidad. Pendiente por ejecutar durante este año pruebas anuales de ingeniería social orientadas a verificar aspectos de protocoles internos de seguridad, nivel de concientización de los funcionarios y terceros que laboren en la entidad sobre temas de seguridad de la información, conocimiento y/o cumplimiento de las políticas de seguridad y privacidad de la información de la entidad y nivel de exposición de la información publicada en internet de la entidad y de sus empleados	Ninguna.

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	EVIDENCIAS
Implementación del plan de tratamiento de riesgos.	Existe un documento con el plan de tratamiento de riesgos e incidentes, y se ha ejecutado de cierta forma, realizando un trato correspondiente a lo que pueda producirse en relación de la seguridad y privacidad de la información. Documento con el plan de gestión de incidentes.	Documento 16 - Riesgos Identificados y Valorados de acuerdo a la Metodología. Documento 15 - Gestión de Incidentes de la Gobernación de N.de.S.
Indicadores De Gestión.	Documento pendiente con la descripción de los indicadores de gestión de seguridad y privacidad de la información. Que sirve para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad.	Ninguna.
Plan de Transición de IPv4 a IPv6	Se realizó plan de diagnóstico y transición de IPV4 a IPV6, quedando pendiente su implementación.	Documento 17 – Diagnostico y Transición de IPV4 a IPV6

4.5. FASES IV: EVALUACION DE DESEMPEÑO

El objetivo de esta fase es evaluar el desempeño y la eficacia del MGPI, a través de instrumentos que permita determinar la efectividad de la implantación del MSPI.

Figura 5 - Fase de Evaluación de desempeño

Tabla 5. Metas, Resultados e Instrumentos de la de la fase de evaluación de desempeño

EVALUACION DEL DESEMPEÑO			
METAS	**RESULTADOS**	**INSTRUMENTO MSPI**	**MRAE**
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Guía No 16 – Evaluación del desempeño.	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 15 – Guía de Auditoría.	

SITUACION ACTUAL DE GOBERNACION N.D.S EN FASE DE EVALUACION DEL DESEMPEÑO

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	EVIDENCIAS
Plan de revisión y seguimiento, a la implementación del MSPI.	Pendiente elaboración de documento con el plan de seguimiento evaluación y análisis del modelo de seguridad revisado y aprobado por Dirección.	Ninguna
Plan de Ejecución de Auditorias	Pendiente la ejecución de auditorías del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, estas se deberán llevar a cabo para la revisión del modelo de seguridad de la información y ciberseguridad implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del modelo de seguridad cumplan con los requisitos establecidos en la Norma ISO 27002:2013.	Ninguna

4.6. FASES V: MEJORA CONTINUA

El objetivo de esta fase es consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el modelo de seguridad.

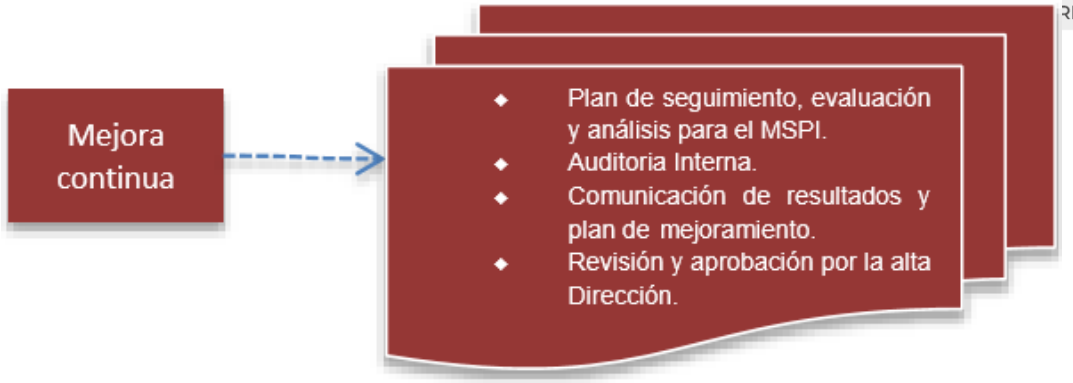

Figura 6 - Fase de mejoramiento continúo

Tabla 6. Metas, Resultados e Instrumentos de la de la fase de mejora continua

MEJORA CONTINUA			
METAS	**RESULTADOS**	**INSTRUMENTOS MSPI**	**MRAE**
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15

SITUACION ACTUAL DE GOBERNACION N.D.S EN FASE DE MEJORA CONTINUA

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	EVIDENCIAS
Plan de mejora continua	Pendiente **Diseñar** el **plan de mejoramiento continuo de seguridad** y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el Sistema de Gestión de Seguridad y Privacidad de la Información de la Gobernación de Norte de Santander, que cumplan con los requisitos establecidos en la Norma ISO 27002:2013. Y luego proceder a comunicar resultados.	Ninguna

5. NIVEL DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Al implementar herramienta de autodiagnóstico INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD SOCIALIZADO POR EL AREA DE Gobierno Digital de MINTIC, nos permite identificar el nivel de madurez del MSPI en el que se encuentra la entidad, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado.

Figura 7 - Diferentes niveles que hacen parte del modelo de madurez.

SITUACION ACTUAL DE NIVEL DE MADUREZ DE LA GOBERNACION N.D.S.

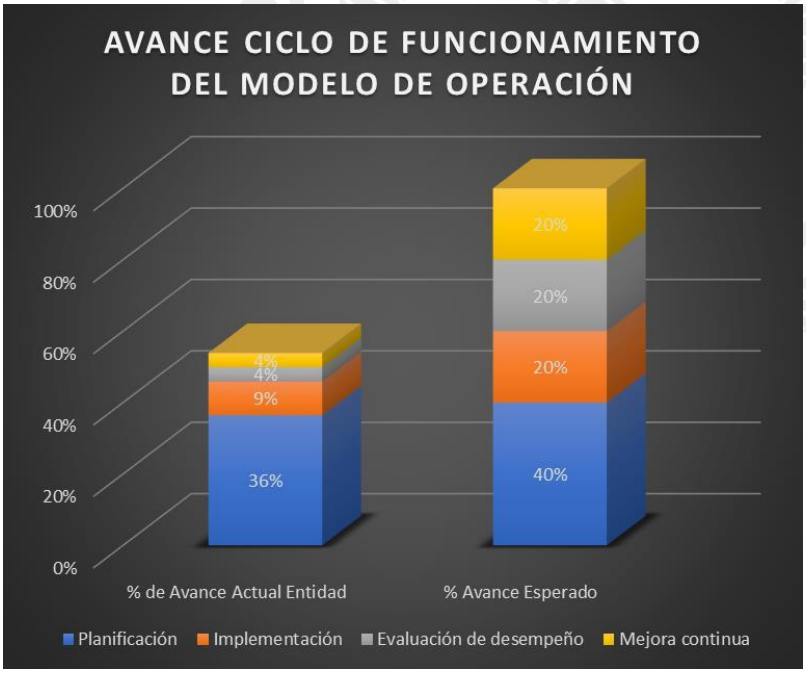

Figura 8 – Avance Actual del Ciclo del PHVA del Modelo de Seguridad y Privacidad de la Gobernación de N.de.S..

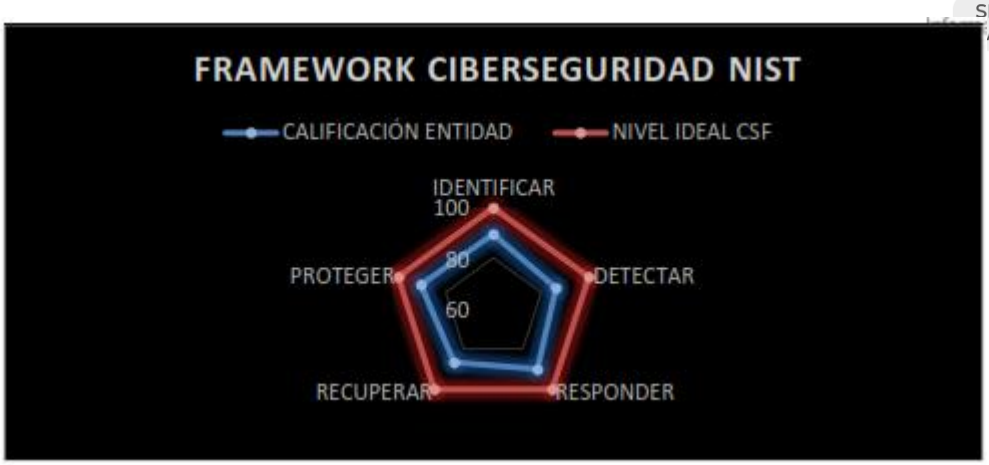

Figura 9 – Calificación frente a mejores prácticas en cuanto a Ciberseguridad del Modelo de Seguridad y Privacidad de la Gobernación de N.de.S..

En conclusión, se puede referenciar que la Gobernación de Norte de Santander, luego de su diagnóstico, se encuentra en la etapa de nivel de madurez **DEFINIDO,** donde se puede resaltar que:

- ✓ La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la
- ✓ seguridad de la información.
- ✓ La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la
- ✓ información.
- ✓ La Entidad ha establecido formalmente políticas de Seguridad de la información y estas
- ✓ han sido divulgadas.
- ✓ La Entidad tiene procedimientos formales de seguridad de la Información
- ✓ La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la
- ✓ información.
- ✓ La Entidad ha realizado un inventario de activos de información aplicando una
- ✓ metodología.
- ✓ La Entidad trata riesgos de seguridad de la información a través de una metodología.
- ✓ Se implementa el plan de tratamiento de riesgos.
- ✓ La entidad cuenta con un plan de transición de IPv4 a IPv6.

6. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Figura 8 – Brecha por Controles o Dominios de la Gobernación N.de.S., según Norma ISO 27001:2013

7. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2024 – 2025 se definen las siguientes actividades para el mejoramiento de la Seguridad y Privacidad de la información las cuales se encuentran enmarcadas en la Política de Seguridad y Privacidad de la Información y en los Lineamientos de la Estrategia de Gobierno Digital (GD) de la Gobernación de Norte de Santander – Más Oportunidades para Todos.

Actividad	Segundo Semestre 2024	Primer Semestre 2025
Evaluar la criticidad de los contratos del recurso tanto humano como tecnológico.	X	
Crear y aplicar encuesta de diagnóstico de seguridad y privacidad de la información	X	
Crear el procedimiento de control documental del MSPI	X	

Actividad	Segundo Semestre 2024	Primer Semestre 2025
Incluir en la Gestión de proyectos la Política de seguridad y privacidad de la Información	X	
Realizar inventario de partes externas o terceros a los que se transfiere información de la Gobernación de Norte de Santander	X	
Realizar formato de acuerdo de transferencia de información	X	
Implementar la Política de Teletrabajo de la Gobernación de Norte de Santander	X	
Realizar inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden		X
Realizar y/o crear listado de auditorías relacionadas con seguridad de la información realizada en la Gobernación de Norte de Santander.		X
Definir indicadores y métricas de seguridad de la información.		X
Definir la declaración de aplicabilidad de la entidad.		X
Crear y/o desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información de la Gobernación de Norte de Santander		X
Aplicar y actualizar la Política de Seguridad y Privacidad de la Información.	X	X
Aplicar y actualizar el Plan de Gestión de incidentes.	X	X
Aplicar y actualizar el Plan de Tratamiento de Riesgos de Seguridad Digital.	X	X

Actividad	Segundo Semestre 2024	Primer Semestre 2025
Aplicar y actualizar el Plan de Gestión de Riesgos de Seguridad Digital.	X	X

8. TERMINOS Y REFERENCIAS

Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.
Amenaza: Es la causa potencial de un daño a un activo de información.
Anexo SL: Nuevo esquema definido por International Organization for Standardization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado "Anexo SL", que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.
Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.
Causa: Razón por la cual el riesgo sucede.
Ciberiesgo o riesgo cibernético: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos. [CE 007 de 2018 SFC].
Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de FINDETER. [CE 007 de 2018 SFC].
Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.
Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.
Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados
Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.
Disponibilidad: Propiedad de determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.
Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.
Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.
Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.
Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.
Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.
Responsables del Activo: Personas responsables del activo de información.
Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.
Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.
PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.
SARC: Siglas del Sistema de Administración de Riesgo Crediticio.

SARL: Siglas del Sistema de Administración de Riesgo de Liquidez.
SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.
SARO: Siglas del Sistema de Administración de Riesgos Operativos.
Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).
SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.
Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.
Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

SECRETARIA DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES
GOBERNACION DE NORTE DE SANTANDER