



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



DEPARTAMENTO DEL META



EL META
Tierra de Oportunidades
Inclusión, Reconstrucción y Equidad



IDERMETA

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 1 de 14

CONTENIDO

INTRODUCCIÓN	2
OBJETIVO GENERAL.....	3
OBJETIVOS ESPECIFICOS	3
METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD	4
CICLO OPERACIÓN	4
FASE I: DIAGNOSTICO.....	5
FASES II: PLANIFICACION	6
FASE III: IMPLEMENTACIÓN.....	9
FASE IV: EVALUACIÓN DE DESEMPEÑO	11
FASE V: MEJORA CONTINUA.....	11
PLAN DE IMPLEMENTACIÓN MODELO DE SEGURIDAD.....	13

	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 2 de 14

INTRODUCCIÓN

El Instituto de Deporte y Recreación del Meta es consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciones legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del Instituto, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada. En la medida que las organizaciones tenga una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas.

Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riesgos que pueden afectar su seguridad, con el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información. Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información y la protección y privacidad de los datos, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de seguridad de la información basado

	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 3 de 14

en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto del negocio como de sus partes interesadas.

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información del Instituto de Deporte y Recreación del Meta, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno en Línea, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad y Privacidad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información del Instituto de Deporte y Recreación del Meta, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos del instituto y en cumplimiento de las disposiciones legales vigentes.

OBJETIVOS ESPECIFICOS

- Mediante la utilización del Modelo de Seguridad y Privacidad contribuir al incremento de la transparencia en la gestión pública.
- Definir las etapas para establecer la estrategia de seguridad de la entidad.
- Implementar el Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Línea.
- Establecer los lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 4 de 14

METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD

CICLO OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.



Figura 1. Ciclo de operación Modelo de Seguridad y Privacidad de la Información
Fuente: <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

Fase Diagnóstico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

Fase Planificación (Planear): 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 (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 5 de 14

Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

Fase Mejora Continua (Actuar): 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.

FASE I: DIAGNOSTICO

Identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

METAS	ACTIVIDADES
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.
Identificar el nivel de madurez de seguridad y privacidad de la 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 la estrategia de Gobierno en Línea.
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 de la entidad y definición de planes de mitigación.

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTES Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 6 de 14

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

FASES II: PLANIFICACION

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.

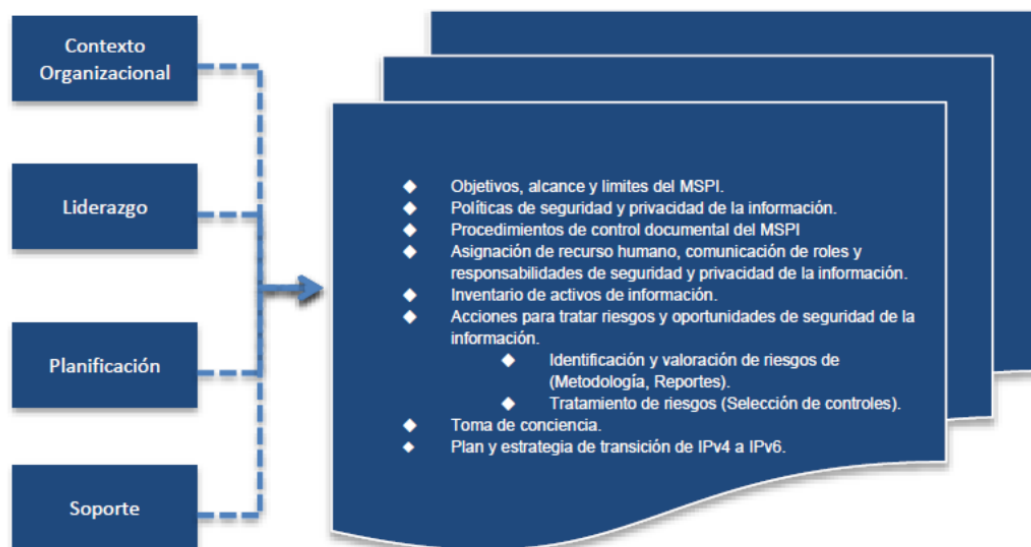


Figura 3. Fase de planificación modelo de seguridad

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 7 de 14

METAS	ACTIVIDADES
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información.	Realizar un Análisis de Contexto de la entidad entorno a la seguridad de la información con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.
Definir el alcance del SGSI de la entidad	Definir el alcance del Sistema de Gestión de Seguridad de la Información 'SGSI' de la entidad aprobado por la Alta Dirección y socializado al interior de la Entidad. Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	Definir un marco de gestión que contemple roles y responsabilidades para la implementación, administración, operación y gestión de la seguridad de la información en la entidad. Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad pertinentes a la seguridad de la información.
Definir la metodología de riesgos de seguridad de la información	Definir Metodología de Valoración de Riesgos de Seguridad. Integrar la metodología definida con la metodología de riesgos operativos de la entidad. Implementar un sistema de información para la administración y gestión de los riesgos de seguridad de la entidad.
Elaborar las políticas de seguridad y privacidad de la	Elaborar Política General de Seguridad y Privacidad la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad. Elaborar el manual

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 8 de 14

información de la entidad	de Políticas de Seguridad y Privacidad de la Información, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad.
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información	• Elaborar los documentos de operación del sistema de seguridad de la información, tales como: • Declaración de aplicabilidad • Procedimiento y/o guía de identificación y clasificación de activos de información. • Procedimiento para control de documentos (SGI) • Procedimiento para auditoría interna (SGI) • Procedimiento para medidas correctivas (SGI) • Procedimiento para la gestión de eventos e incidentes de seguridad de la información • Procedimiento para la gestión de vulnerabilidades de seguridad de la información
Identificar y valorar activos de información	Realizar la identificación y valoración de los activos de información de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del SGSI. Documentar el inventario de activos de información de la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la	Realizar la identificación y valoración de los riesgos transversales de seguridad de la información y definir los respectivos planes de tratamiento. Realizar la

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTE Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 9 de 14

información de la entidad	valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI. Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos.
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.	Elaborar plan anual de capacitación y sensibilización anual de seguridad de la información
Establecer Plan de diagnóstico de IPv4 a IPv6	Realizar el diagnóstico para la transición de la entidad de IPv4 a IPv6. Documentar el Plan de diagnóstico para la transición de IPv4 a IPv6.

FASE III: IMPLEMENTACIÓN

Llevar acabo la implementación de la fase de planificación del SGSI, 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 modelo de seguridad
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 10 de 14

METAS	ACTIVIDADES
Establecer el plan de implementación de seguridad de la información	Implementar el plan de implementación del modelo de seguridad y privacidad de la información el cual debe ser revisado y aprobado por el comité de riesgos
Ejecutar el plan de tratamiento de riesgos	Ejecutar el plan de tratamiento de los riesgos transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riesgos
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.	Ejecutar plan de transición a IPv6 y elaborar informe de implementación.
Establecer indicadores de gestión de seguridad	Definir los indicadores 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.
Implementar procedimiento de gestión de eventos e incidentes de seguridad	Implementar el procedimiento y los mecanismos para la gestión de los eventos e incidentes de seguridad de la información.
Implementar procedimiento de gestión de vulnerabilidades	Implementar el procedimiento y los mecanismos para la gestión de vulnerabilidades seguridad de la información.
Ejecutar pruebas anuales de vulnerabilidades e intrusión	Ejecutar el plan anual de capacitación, socialización y sensibilización de seguridad de la información del Instituto.

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTES Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 11 de 14

FASE IV: EVALUACIÓN DE DESEMPEÑO

Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.



Figura 5. Fase Evaluación Desempeño modelo de seguridad

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

METAS	ACTIVIDADES
Ejecución de auditorías de seguridad de la información	Ejecución de auditorías del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoría revisado y aprobado por la Alta Dirección.
Plan de seguimiento, evaluación y análisis de SGSI	Elaboración documento con el plan de seguimiento, evaluación y análisis del SGSI revisado y aprobado por el Comité Institucional de Gestión y Desempeño.

FASE V: MEJORA CONTINUA

Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la

 IDERMETA INSTITUTO DEPARTAMENTAL DE DEPORTES Y RECREACIÓN DEL META	PROCESO SEGURIDAD DE LA INFORMACIÓN		
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
Versión: 01	Emisión y vigencia: 28-01-2019	Código: SI-PSP-001	Página 12 de 14

información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI

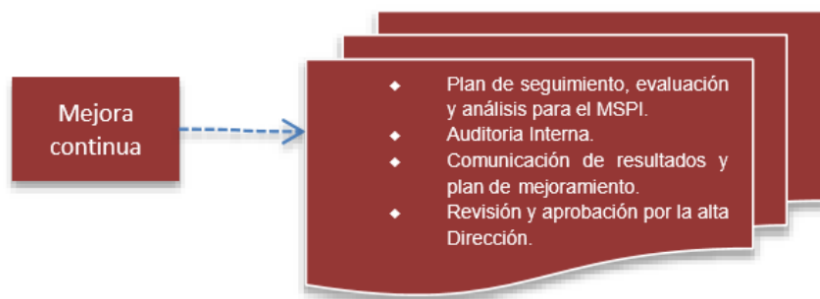


Figura 6. **Fase Mejora Continua modelo de seguridad**

Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea

METAS	ACTIVIDADES
Diseñar plan de mejoramiento	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 de la Información.

INSTITUTO DE DEPORTE Y RECREACIÓN DEL META																																																
PLAN DE IMPLEMENTACIÓN MODELO DE SEGURIDAD																																																
ACTIVIDAD	Febrero				Marzo				Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre				Noviembre				Diciembre							
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4				
FASE DIAGNOSTICO																																																
Determinar el estado actual de la gestión de seguridad de la entidad																																																
Identificar el nivel de madurez de seguridad de la entidad																																																
Identificar vulnerabilidades técnicas																																																
FASE PLANIFICACIÓN																																																
Realizar análisis de Contexto de la Entidad en torno a la seguridad.																																																
Definir el alcance del SGSI de la entidad																																																
Definir Roles y Responsables de seguridad de la información																																																
Definir la metodología de riesgos de seguridad de la información																																																
Elaborar políticas de seguridad y privacidad de la información																																																
Elaborar documentación de operación del sistema de seguridad																																																
Identificar y valorar activos de información																																																
Identificar y valorar los riesgos de seguridad de la información																																																
Definir plan de capacitación, comunicación y sensibilización																																																
Diagnóstico Plan de IPv4 a IPv6																																																
FASE IMPLEMENTACIÓN																																																
Implementar planes de acción resultado de las auditorias																																																
Ejecutar plan de tratamiento de riesgos																																																
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.																																																
Implementar procedimiento de gestión de eventos e incidentes de seguridad																																																
Implementar procedimiento de gestión de vulnerabilidades																																																
Ejecutar plan de capacitación y sensibilización de seguridad																																																
FASE EVALUACIÓN DESEMPEÑO																																																
Ejecución auditoria de seguridad de la información																																																
FASE MEJORA CONTINUA																																																
Diseñar plan de mejoramiento																																																