

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011,

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, deberán integrar los planes institucionales y estratégicos y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

LOTERIA DE MEDELLIN

2026

Aprobado el 28 de enero de 2026, mediante Acta N°4 del Comité Institucional de Gestión y Desempeño

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

TABLA DE CONTENIDO

INTRODUCCIÓN	3
1. DEFINICIONES	4
2. OBJETIVOS	6
Objetivo General	6
Objetivos Específicos	6
3. ALCANCE.....	6
4. MARCO NORMATIVO	6
5. LÍNEA BASE.....	7
6. METODOLOGÍA.....	9
7. DESARROLLO DEL PLAN.....	9
Etapa 1	10
Etapa 2	11
Etapa 3	11
9. CRONORAMA DE ACTIVIDADES	11
10. MEDICIÓN - INDICADOR	12
11. SEGUIMIENTO AL PLAN:.....	13
12. ESTRATEGIAS DE DIFUSIÓN	13
13. BIBLIOGRAFIA.....	13

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

INTRODUCCIÓN

A través del Plan de Seguridad y Privacidad de la información para el cuatrienio 2024-2027, Lotería de Medellín expone a la comunidad el propósito de seguir avanzando en la implementación de controles tanto administrativos como técnicos que garanticen altos niveles de protección de la información contra factores que pongan en riesgo su integridad, disponibilidad y confidencialidad.

Con la formulación y ejecución de este plan, también se le da cumplimiento a la normatividad establecida por el Gobierno Nacional para todas las entidades públicas, en especial al Decreto 1008 de 2018 que formula la política de Gobierno Digital donde el Modelo de Seguridad y la Privacidad de la Información (MSPI) es uno de los 3 habilitadores transversales.



Ilustración 1. La seguridad y privacidad como habilitador transversal de Gobierno Digital.

Este modelo nace a partir del sistema de gestión de seguridad de la información expuesto a través de la norma internacional ISO 27001, al cual lo complementa la Ley 1581 de 2012 sobre protección de datos personales.

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

A partir de los resultados obtenidos en un ejercicio de autodiagnóstico, el cual se midió usando la herramienta proporcionada por Mintic, se identificaron las líneas de acción y las respectivas tareas que la entidad deberá llevar a cabo para lograr el propósito de implementar el MSPI.

El presente documento actualiza y expone las principales líneas de acción a ser llevadas a cabo en la vigencia 2026.

1. DEFINICIONES

- **Disponibilidad.** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A grandes rasgos, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.
- **Integridad.** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas (No es igual a integridad referencial en bases de datos.) A grandes rasgos, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Confidencialidad.** La confidencialidad es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
- **Riesgo.** Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Amenaza.** Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Vulnerabilidad.** Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad.** Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

- **Impacto.** Son las consecuencias que genera un riesgo una vez se materialice.
- **Control o Medida.** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **Activo.** Cualquier elemento que tenga valor para la organización.
- **Análisis del riesgo.** Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- **Causa.** Elemento específico que origina el evento.
- **Contexto externo.** Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- **Contexto interno.** Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- **Controles.** Procesos, políticas y/o actividades que pueden modificar el riesgo.
- **Criterios de riesgos.** Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- **Evaluación del Riesgo.** Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- **Evento.** Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- **Fuente.** Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; la fuente del riesgo puede ser tangible o intangible.
- **Gestión del riesgo.** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del riesgo.** Se determinan las causas, fuentes del riesgo y los eventos con base al contexto del proceso, que pueden afectar el logro de los objetivos del mismo.

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

- **Consecuencia.** Es el resultado de que se materialice un riesgo, pueden existir niveles de consecuencias.

2. OBJETIVOS

Objetivo General

- Documentar y ajustar el Modelo de Seguridad y Privacidad de la Información durante la vigencia 2026 de acuerdo con los lineamientos establecidos en el programa de Gobierno Digital del Gobierno Nacional.

Objetivos Específicos

- Definir el plan de acción para que la Lotería de Medellín se pueda ajustar al modelo de seguridad y privacidad de la información de acuerdo con los lineamientos establecidos en el programa de Gobierno Digital del Gobierno Nacional.
- Alinear las acciones en Seguridad y Privacidad de la información con el Plan Estratégico de la Oficina de las TIC y con el Plan Estratégico de la entidad para el año 2026.
- Fortalecer la apropiación, conocimiento y buenas prácticas en Seguridad y Privacidad de la información por parte de los miembros de la entidad durante la vigencia del presente plan.

3. ALCANCE

El Plan de Seguridad y Privacidad pretende implementar los controles incluidos en el Modelo de Seguridad y Privacidad de la Información formulado por el Ministerio de las TICs (Mintic) que apliquen a la Lotería de Medellín.

4. MARCO NORMATIVO

- **Decreto 1008.** 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

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital.
- **Modelo de Seguridad y Privacidad de la Información – MSPI.** Incorporado en la Política de Gobierno Digital.
- **Familia de normas NTC / ISO27000.** Normas colombianas ICONTEC correspondientes a las respectivas normas ISO sobre Seguridad de la Información.

5. LÍNEA BASE

La seguridad de la información, entendida desde la norma ISO 27001 tiene 3 aristas o aspectos fundamentales, a los controles incluidos en el MSPI: Disponibilidad, Integridad y Confidencialidad.



Ilustración 2.

Fuente. As.Net – Seguridad de la información(<http://www.asnetla.com/inicio/seguridad/>). Tomada el 6 de octubre de 2020.

Para la protección de estos, en la mayoría de organizaciones están involucrados las personas, los procesos y una plataforma tecnológica, los cuales mediante el ciclo PHVA logran establecer y estandarizar los controles adecuados para garantizar altos niveles de protección de la seguridad y la privacidad.

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

El conjunto de controles de la ISO27001 está agrupado en 14 categorías que se clasifican en 2 grandes grupos: Administrativas y Técnicas.

Como su nombre lo indica, los controles administrativos están orientados a las acciones que la organización implementa a través de procedimientos organizativos de gestión por parte del personal de la entidad, e incluyen la asignación de roles y responsabilidades en seguridad, la documentación de las políticas y la participación de todas las áreas o dependencias.

Por su parte, los controles técnicos incorporan mecanismos tecnológicos y de infraestructura física (locativa, eléctrica, etc).

Lotería de Medellín realizó un diagnóstico del nivel de madurez de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante el cual se obtuvo un 54,00% de avance.

Tabla 1. Diagnóstico del nivel de madurez de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	60	100	EFFECTIVO
A.8	GESTIÓN DE ACTIVOS	43	100	EFFECTIVO
A.9	CONTROL DE ACCESO	58	100	EFFECTIVO
A.10	CRIPTOGRAFÍA	50	100	EFFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	48	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	50	100	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	58	100	EFFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	56	100	EFFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34	100	REPETIBLE
A.18	CUMPLIMIENTO	54	100	EFFECTIVO
	PROMEDIO EVALUACIÓN DE CONTROLES	54	100	EFFECTIVO

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

6. METODOLOGÍA

La metodología de Mintic está expuesta a través de un conjunto de documentos que están publicados en el link: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>.

A partir del diagnóstico realizado, en el cual se estableció un nivel de madurez de cada una de las categorías, se identifican las tareas a realizar, siguiendo las guías mencionadas.

Con el objetivo de obtener y presentar logros tempranos, se ha establecido una meta parcial inicial de al menos un 70% de madurez del modelo, lo que representa un nivel aceptable en el manejo de la seguridad de la información por parte de la entidad. Para lograr este nivel se debe garantizar que todos los controles que le apliquen a la entidad deberán estar implementados, socializados y documentados.

En una etapa posterior, se deberá avanzar en el monitoreo permanente a los controles adoptados y estos deberán formar parte de las buenas prácticas de todas las dependencias, empleados, proveedores, distribuidores, y demás grupos de interés.

7. DESARROLLO DEL PLAN

En el Plan de Implementación del MSPI se establecieron 3 etapas para su desarrollo. En la etapa 1 la entidad estará terminando de implementar los controles en seguridad de tal manera que se logre en el primer semestre de 2026 un nivel aceptable con las políticas y procedimientos debidamente documentados y socializados. En la etapa 2, que corresponde al semestre 2 del año 2026, se implementarán mecanismos de evaluación y desempeño a cada uno de los controles y mecanismos, además de convertir cada uno de estos en buenas prácticas cotidianas. La etapa 3 estará orientada al mejoramiento continuo de acuerdo con los lineamientos de la fase 4 de la guía de seguridad y privacidad de la información de MINTIC.

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

Tabla 2. Etapas para el desarrollo del Plan de Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Etapas	2026/Semestre 1	2026/Semestre 2	2026/Semestre 2
Etapas1	Seguimiento y Ajustes de controles implementados		
Etapas2		Evaluación y Desempeño	
Etapas3			Mejoramiento Continuo

Etapas 1

En la tabla 3 se presenta las principales acciones que ejecutarán durante el año 2026 para la primera etapa y así lograr el nivel de al menos un 83% o superior de madurez del MSPI.

Durante la vigencia 2026 se definirán, documentarán e implementarán los controles para los siguientes dominios, teniendo en cuenta las directrices definidas en el Anexo A de la norma ISO 27001:2022, así:

Tabla 3. Acciones a ejecutar durante el año 2026 para la primera etapa.

N°	Dominio	Etapas 1 2026
A.5	Políticas de seguridad de la información	X
A.6	Organización de la seguridad de la información	X
A.7	Seguridad de los recursos humanos	X
A.8	Gestión de activos	X
A.9	Control de acceso	X
A.10	Criptografía	X
A.11	Seguridad física y del entorno	X
A.12	Seguridad de las operaciones	X
A.13	Seguridad de las comunicaciones	X
A.14	Adquisición, desarrollo y mantenimiento de sistemas	X
A.15	Relaciones con los proveedores	X
A.16	Gestión de incidentes de seguridad de la información	X
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	X
A.18	Cumplimiento	X

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

Etapa 2

Una vez tengamos implementados los controles identificaremos los mecanismos para su correspondiente evaluación y desempeño.

Etapa 3

Se desarrollará la fase de mejoramiento continuo del modelo de seguridad y privacidad de la información.

8. PRESUPUESTO

RECURSOS	VARIABLE
Humanos	- Grupo de profesionales internos de seguridad e infraestructura de la Oficina TIC. - Profesionales especialistas en seguridad. - Líderes de procesos. - Jefe de la oficina TIC.
Técnicos	- política de seguridad de MINTIC. - Autodiagnóstico de seguridad – MINTIC. - MSPI. - Guía para la administración del riesgo y el diseño de controles en entidades públicas. - Norma ISO 27001:2022 - Herramienta para la gestión de riesgos (Lotería de Medellín y función pública).
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	- Recursos humanos y técnicos para la revisión, estructuración, implementación de controles, adquisición de herramientas de seguridad, elaboración y actualización de políticas. - Presupuesto estimado: \$ 877.491.603

9. CRONORAMA DE ACTIVIDADES

Ver Plan de Acción Integral.

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

	FORMATO			CÓDIGO	
	GESTIÓN ESTRATÉGICA			VERSION 01	
	PLAN DE ACCION INTEGRAL 2026			FECHA: 13/jul /2023	
PLAN	Objetivo	1. Generar más recursos a la salud.	INDICADOR DE ESTRUCTURA, PROCESO Y RESULTADO	Entregable	Responsabl
12. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Documentar y ajustar el Modelo de Seguridad y Privacidad de la Información durante la vigencia 2026 de acuerdo con los lineamientos establecidos en el programa de Gobierno Digital del Gobierno Nacional.	Autodiagnostico	(Avance Proyecto / Avance planeado Proyecto) x 100	Autodiagnostico MSPi	GESTION TI
		Definir controles carentes de acuerdo a los resultados del autodiagnostico			
		Documentar controles			
		Implementar controles			
		Identificar mecanismos de monitoreo			
		Definir mecanismos de monitoreo			

[illegible]

10. MEDICIÓN - INDICADOR

Indicador	Tipo de Indicador	Formula del Indicador	Responsable	Seguimiento
% de cumplimiento del cronograma proyectos PSPI	Eficacia	(Avance Actividades PSPI/ Avance planeado Actividades PSPI) x 100	Oficina de las TICS	Trimestral

Avance de los indicadores proyectados para el año 2026.

	FORMATO	CODIGO F-GE-018
	GESTIÓN ESTRATÉGICA	VERSIÓN 02
	PLANES INSTITUCIONALES	FECHA: 13/ene./2026

11. SEGUIMIENTO AL PLAN:

Para este numeral se realiza el seguimiento al Plan de Seguridad y Privacidad de la Información con el plan de acción vigencia 2026 donde se reporta los avances en indicadores, estado de avance de los proyectos, de igual manera en la ejecución de los proyectos asignados en el plan de realiza un control trimestral del estado actual.

12. ESTRATEGIAS DE DIFUSIÓN

El al Plan de Seguridad y Privacidad de la Información como documento que expone parte de la estrategia de la Oficina de TI, debe ser comunicado a toda la entidad, iniciando con la divulgación a nivel directivo, para después dar a conocer a las diferentes áreas de la entidad.

Como parte del proceso de divulgación del Plan de Seguridad y Privacidad de la Información se indican las actividades a realizar:

- Elaboración de presentación a los directivos de la entidad.
- Publicación del Plan de Seguridad y Privacidad de la Información en el sitio web de la Lotería de Medellín.
- Divulgación vía correo corporativo.
- Capacitación a los terceros de interés en los aspectos fundamentales del Plan de Seguridad y Privacidad de la Información.

13. BIBLIOGRAFIA

- Norma técnica colombiana NTC-ISO/IEC de la familia 27000
- Guía sobre Seguridad y Privacidad de la Información (<https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>)