	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 TRATAMIENTO DE RIESGOS 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

TABLA DE CONTENIDO

INTRODUCCIÓN 3

1. DEFINICIONES 3
2. OBJETIVOS 5

Objetivo General 5

Objetivos Específicos 5

3. ALCANCE 6
4. MARCO NORMATIVO 7
5. SITUACIÓN ACTUAL 7
6. DESARROLLO DEL PLAN 12
7. CRONORAMA DE ACTIVIDADES 13
8. MEDICIÓN 14
9. BIBLIOGRAFIA 14

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información recoge la caracterización realizada con anterioridad en la entidad de algunos riesgos de seguridad de la información y ciberseguridad, y busca seguir avanzando en esta ruta usando la metodología establecida en el Manual de Riesgos de la entidad y la Guía de Gestión de Riesgos de Seguridad de Mintic, en concordancia con el Modelo de Seguridad y Privacidad de la Información, mediante la revisión y actualización de los riesgos ya identificados y actualmente tratados, sumándole la identificación, valoración y definición del tratamiento de otros potenciales riesgos. El Plan se complementa con una adecuada documentación, socialización y buenas prácticas, a fin de blindar a la entidad al máximo de la materialización de dichos riesgos a través de la incorporación de los controles asociados a cada uno de estos en los procesos de la entidad. El Plan toma como referencia los estándares mundiales de la familia ISO 27000 e ISO 31000, el Decreto 1008 del14 de junio de 2018 de Gobierno Digital, la guía de Mintic para la gestión de riesgos de seguridad y privacidad de la información, y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital- emitida por el DAFP.

El presente documento compila las acciones que se pretenden realizar 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.

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

2. OBJETIVOS

Objetivo General

- Establecer, implementar y mantener un enfoque sistemático de gestión de riesgos de seguridad de la información durante la vigencia 2026, orientado a identificar, analizar, evaluar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad, en cumplimiento de la normativa aplicable y los lineamientos institucionales.

Objetivos Específicos

- Identificar y clasificar los activos de información y sus riesgos asociados, considerando amenazas, vulnerabilidades e impactos sobre los procesos críticos de la entidad, incluidos los procesos regulados por la NTC 6767:2024.

- Evaluar y priorizar los riesgos de seguridad de la información y ciberseguridad, mediante criterios de impacto y probabilidad, para definir planes de tratamiento que incluyan controles preventivos, detectivos y correctivos.

- Alinear la gestión de riesgos de seguridad y privacidad de la información con el Plan Estratégico de la Oficina de las TIC y el Plan Estratégico Institucional para la vigencia 2026, asegurando su integración con los procesos misionales y de apoyo.

- Implementar y fortalecer los controles del Sistema de Gestión de Seguridad de la Información (SGSI) basados en ISO/IEC 27001, orientados a reducir el nivel de riesgo residual a niveles aceptables por la entidad.

- Garantizar el cumplimiento normativo y regulatorio aplicable, incluyendo la legislación colombiana en materia de protección de datos personales, seguridad de la información y los requisitos establecidos por la NTC 6767:2024 para los procesos de sorteo y presorteo.

- Promover la cultura organizacional en gestión del riesgo y seguridad de la información, fortaleciendo la capacitación, concienciación y responsabilidades del personal frente a la identificación y reporte de eventos e incidentes de seguridad.

- Monitorear y medir la eficacia de los controles de seguridad, mediante indicadores, auditorías internas y revisiones periódicas, que permitan evidenciar la mejora continua del modelo de gestión de riesgos de seguridad de la información.

3. ALCANCE

El presente plan hace parte del Plan de Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y le aporta a este el tratamiento que la entidad debe realizar a los riesgos de seguridad y ciberseguridad que se identifiquen y valoren de acuerdo con las guías que se referencian en el marco de referencia.

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 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.
- NTC / ISO27005:2022. Gestión del Riesgo, Principios y Directrices.
- NTC 6767:2024. Juegos de azar territoriales

5. SITUACIÓN ACTUAL

Actualmente, la Lotería de Medellín gestiona los riesgos asociados a la Seguridad y Privacidad de la Información y ciberseguridad mediante una Matriz de Riesgos de Seguridad y Privacidad de la Información, integrada al Sistema de Gestión de Calidad y articulada con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Sistema de Gestión de Seguridad de la Información (SGSI).
La matriz contempla la identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos que afectan los activos de información, los procesos misionales, estratégicos y de apoyo, así como los sistemas de información y la infraestructura tecnológica de la entidad, incluyendo aquellos asociados a los procesos de sorteo y presorteo regulados por la NTC 6767:2024.

Los riesgos son estructurados considerando como mínimo los siguientes elementos: activo de información, amenaza, vulnerabilidad, impacto, probabilidad, nivel de riesgo inherente, controles existentes, plan de tratamiento, responsable y nivel de riesgo residual.

El conjunto de riesgos gestionados es de carácter dinámico y evolutivo, y se actualiza de manera periódica como resultado de:

- Procesos de identificación y reevaluación de riesgos
- Auditorías internas y externas
- Gestión de incidentes de seguridad de la información
- Cambios en los procesos, tecnologías o proveedores
- Actualizaciones normativas y regulatorias aplicables

La siguiente tabla presenta el resumen de los riesgos priorizados vigentes, de acuerdo con los criterios de aceptación y tolerancia al riesgo definidos por la alta dirección, conforme a la versión vigente del archivo Matriz_Riesgos_Seguridad.xls

Tabla 1. Resumen de lo riesgos más relevantes asociados a la Seguridad y Privacidad de la información

DESCRIPCIÓN DEL RIESGO	CAUSA INMEDIATA	CAURA RAIZ	FACTOR DEL RIESGO
Posibilidad de **pérdida** económica y/o reputacional por falta de confidencialidad en la autenticación de un usuario no autorizado, debido al uso de cuentas predeterminadas con privilegios de administrador.	falta de confidencialidad en la autenticación de un usuario no autorizado	debido al uso de cuentas predeterminadas con privilegios de administrador	Económico y/o reputacional
Posibilidad de pérdida económica y/o reputacional por falta de disponibilidad por fallas eléctricas, debido a la falta de redundancia, copia única.	falta de disponibilidad por fallas eléctricas	debido a la falta de redundancia, copia única.	Económico y/o reputacional

DESCRIPCIÓN DEL RIESGO	CAUSA INMEDIATA	CAURA RAIZ	FACTOR DEL RIESGO
Posibilidad de pérdida económica y/o reputacional por falta de confidencialidad en la autenticación de un usuario no autorizado, debido a la falta de formación y conciencia sobre seguridad.	falta de confidencialidad en la autenticación de un usuario no autorizado	debido a la falta de formación y conciencia sobre seguridad.	Económico y/o reputacional
Posibilidad de pérdida económica y/o reputacional por falta de disponibilidad por desastre natural, incendio, inundación, rayo., debido a la falta de redundancia, copia única.	Falta de disponibilidad por desastre natural, incendio, inundación, rayo.	debido a la falta de redundancia, copia única.	Económico y/o reputacional
Posibilidad de pérdida económica y/o reputacional por falta disponibilidad por errores de software, debido a la falta de políticas para el uso de la criptografía.	Falta de disponibilidad por errores de software	debido a la falta de políticas para el uso de la criptografía.	Económico y/o reputacional
Posibilidad de pérdida económica y/o reputacional por falta de confidencialidad por divulgación de contraseñas, debido a una Inadecuada gestión y protección de contraseñas.	Falta de confidencialidad por divulgación de contraseñas	debido a una Inadecuada gestión y protección de contraseñas.	Económico y/o reputacional
Posibilidad de pérdida económica y/o reputacional por falta disponibilidad por errores de software, debido a la	Falta de disponibilidad por errores de software	debido a la configuración incorrecta en políticas de respaldo.	Económico y/o reputacional

DESCRIPCIÓN DEL RIESGO	CAUSA INMEDIATA	CAURA RAIZ	FACTOR DEL RIESGO
Configuración incorrecta en políticas de respaldo.			
Posibilidad de pérdida económica y/o reputacional por falta de confidencialidad en la autenticación de un usuario no autorizado, debido a la falta de cifrado o autenticación en el almacenamiento NFS.	falta de confidencialidad en la autenticación de un usuario no autorizado	debido a la falta de cifrado o autenticación en el almacenamiento NFS	Económico y/o reputacional

6. METODOLOGÍA

El Manual de Riesgos de la entidad clasifica los riesgos en Estratégicos, Operativos, Financieros, de Cumplimiento y Tecnológicos. Debido a que los activos de información están presentes en todos los procesos de la entidad, se parte de la premisa de que los riesgos en Seguridad y Privacidad de la Información están potencialmente asociados al menos a uno de los anteriores tipos de riesgos mencionados.

La metodología que el Manual contempla consiste fundamentalmente en los siguientes pasos, una vez se ha establecido el contexto:

1. Identificación del riesgo.
2. Clasificación del Riesgo.
3. Establecer controles.
4. Aceptación del riesgo.

Esta metodología coincide parcialmente con la propuesta por la norma colombiana NTC27005, la cual, además de los pasos mencionados, incluye algunas actividades adicionales, tales como la comunicación, y el monitoreo y la revisión del riesgo.

Recogiendo ambas metodologías, se propone partir de la documentación actualmente registrada en el sistema de calidad de la entidad, y desarrollar un ciclo para cada riesgo, en el cual se parta de la identificación de este, se realice la respectiva evaluación y documentación y se determinen las tareas a realizar para el tratamiento. Como último paso, si es del caso, determinar el nivel de aceptación del riesgo residual que la entidad asumirá. Todo lo anterior deberá estar acorde con la metodología establecida en la Guía de Gestión de Riesgos de Mintic.

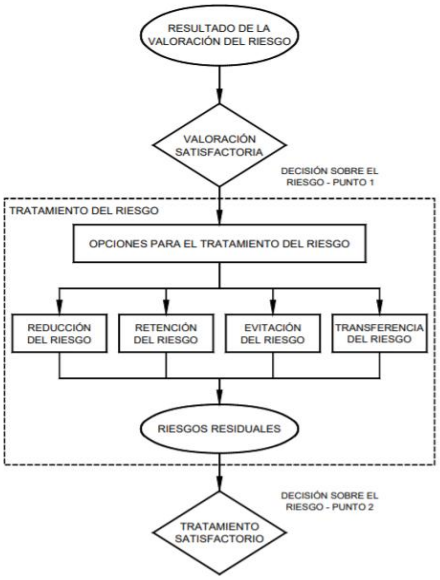


Ilustración 1. Tratamiento del riesgo propuesto por la ISO 27005.

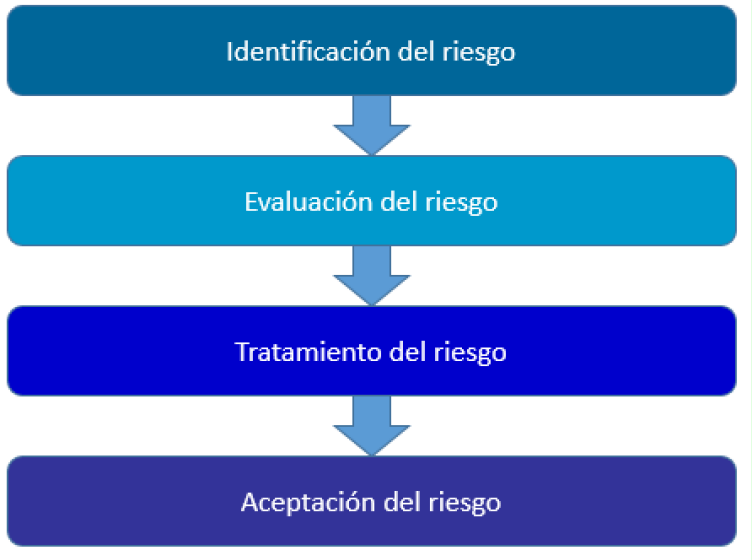


Ilustración 2. Flujo de la metodología que se propone seguir en este plan.

7. DESARROLLO DEL PLAN

El plan de tratamiento de riesgos de seguridad y privacidad de la información se correlacionará con las actividades comprendidas en el plan de seguridad y privacidad de la información y el desarrollo quedará sujeto al desarrollo de la declaración de aplicabilidad a partir de la cual se establecerán las actividades a realizar durante la vigencia.

En la medida en que se vayan identificando y documentando riesgos adicionales, estos deben ser valorados y clasificados de acuerdo con el modelo de gestión del riesgo.

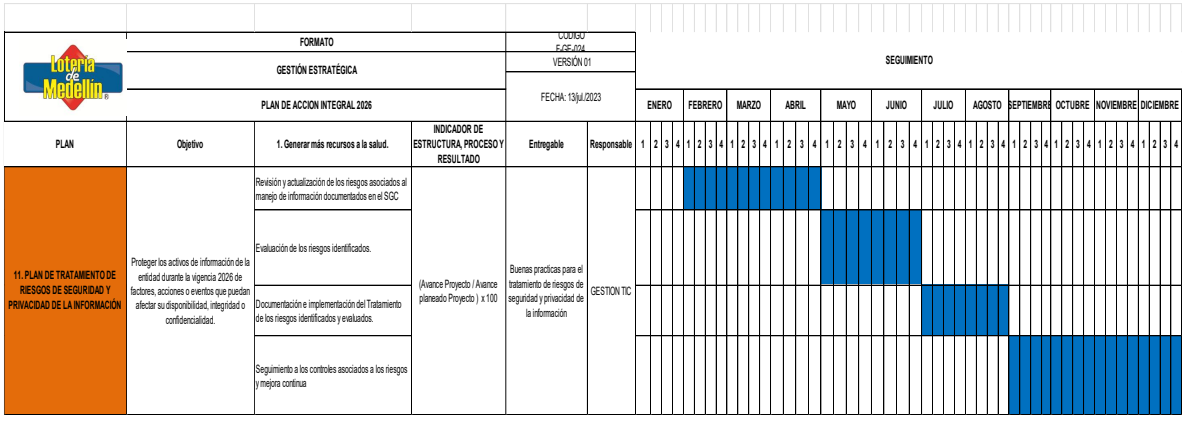
La ejecución de este plan estará alineada con el Sistema de Gestión de Calidad.

8. PRESUPUESTO

RECURSOS	VARIABLE
Humanos	• Grupo de profesionales internos de seguridad e infraestructura de la Oficina TIC. • Profesionales especialistas en seguridad. • Lideres de procesos. • Jefe de la oficina TIC.
Técnicos	• 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 y seguimiento de riesgos. • Presupuesto estimado: $ 183.821.523

9. CRONORAMA DE ACTIVIDADES

Ver Plan de Acción Integral.



FORMATO			CODIGO F-GE-024		
GESTIÓN ESTRATÉGICA			VERSIÓN 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	Responsable
11. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Proteger los activos de información de la entidad durante la vigencia 2026 de factores, acciones o eventos que puedan afectar su disponibilidad, integridad o confidencialidad.	Revisión y actualización de los riesgos asociados al manejo de información documentados en el SGC	(Avance Proyecto / Avance planeado Proyecto) x 100	Buenas practicas para el tratamiento de riesgos de seguridad y privacidad de la información	GESTION TIC
		Evaluación de los riesgos identificados.			
		Documentación e implementación del Tratamiento de los riesgos identificados y evaluados.			
		Seguimiento a los controles asociados a los riesgos y mejora continua			

SEGUIMIENTO

ENERO (1 2 3 4) | FEBRERO (1 2 3 4) | MARZO (1 2 3 4) | ABRIL (1 2 3 4) | MAYO (1 2 3 4) | JUNIO (1 2 3 4) | JULIO (1 2 3 4) | AGOSTO (1 2 3 4) | SEPTIEMBRE (1 2 3 4) | OCTUBRE (1 2 3 4) | NOVIEMBRE (1 2 3 4) | DICIEMBRE (1 2 3 4)

10. MEDICIÓN - INDICADORES

Para el año 2026, se establece el siguiente indicador al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Lotería de Medellín.

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

Avance de los indicadores proyectados para el año 2026.

11. SEGUIMIENTO AL PLAN

El seguimiento al indicador permitirá medir el porcentaje de cumplimiento y se realizará de manera **trimestral.**

12. ESTRATEGIAS DE DIFUSIÓN

Para las estrategias de difusión se realizará por medio de comunicaciones internas, jornadas de sensibilización y concientización en riesgos de seguridad, piezas de comunicación para difundir en la entidad y socializaciones en comité directivo y comité institucional de gestión y desempeño de la Lotería de Medellín.

13. BIBLIOGRAFIA

- Norma técnica colombiana NTC-ISO/IEC27005.
- Guía de gestión de riesgos de Mintic: (https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf).