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 – 2024

Aprobado el 26 enero de 2024, mediante Acta N°2 del Comité Institucional de Gestión y Desempeño

TABLA DE CONTENIDO

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 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 2024.

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.

OBJETIVOS

ObjetivoGeneral

Proteger los activos de información de la entidad durante la vigencia 2024 de factores, acciones o eventos que puedan afectar su disponibilidad, integridad o confidencialidad.

Objetivos Específicos

- Establecer los lineamientos necesarios para el cumplimiento de la legislación colombiana en cuanto a Seguridad y Privacidad de la Información aplicable a la entidad durante la vigencia 2024.

- 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 la vigencia 2024.

- 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 2024.

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 que se identifiquen y valoren de acuerdo con las guías que se referencian en la bibliografía.

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.

SITUACIÓN ACTUAL

Actualmente en el Sistema de Gestión de Calidad de la entidad están caracterizados y documentados 6 riesgos asociados a la Seguridad y Privacidad de la Información. La siguiente tabla expone un resumen de la información allí contenida:

Tabla 1. Resumen de los 6 riesgos asociados a la Seguridad y Privacidad de la Información.

RIESGO	DESCRIPCION	CONTROLES
Acceso inapropiado usuarios internos.	Acceso inapropiado a aplicativos e información por parte de usuarios internos.	Cambio de claves de acceso periódico.
		Política de seguridad.
Acceso inapropiado usuarios externos.	Acceso inapropiado a aplicativos e información por parte de usuarios externos.	Monitoreo periódico.
R29-Perdida de información.	Perdida de información en bases de datos, servidor de archivos y servidores de aplicaciones.	Política de backups.
		Política de seguridad.
		Seguimiento a los documentos contractuales de los contratos de soporte.

R30-Acceso o uso indebido de Internet.	Ataque cibernético.	Seguimiento a los documentos contractuales de los contratos de soporte.
		Política de seguridad.
R65-Uso inadecuado de derechos de autor.	Violación de derechos de autor.	Política de seguridad.
Relaciones con terceros.	Contratos terceros especializados.	Seguimiento a los documentos contractuales de los contratos.
		Política de seguridad de la información.

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.

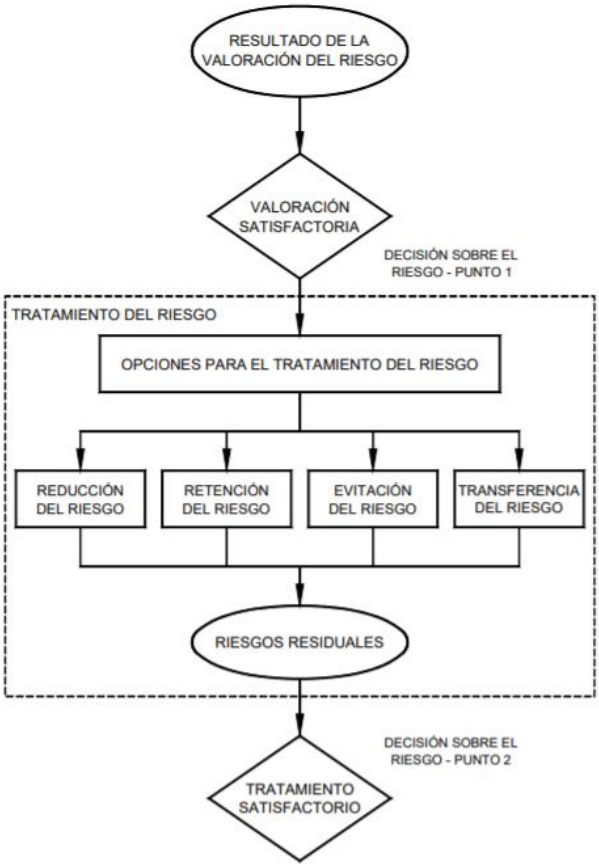


Ilustración 1. Tratamiento del riesgo propuesto por la ISO 27005.

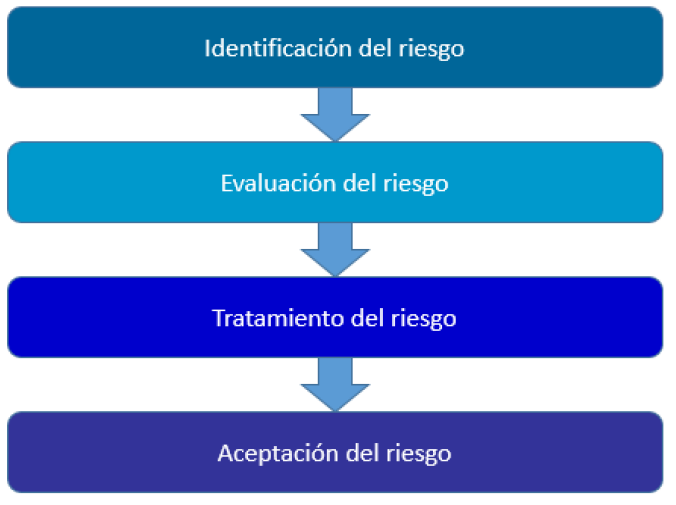


Ilustración 2. Flujo de la metodología que se propone seguir en este plan.

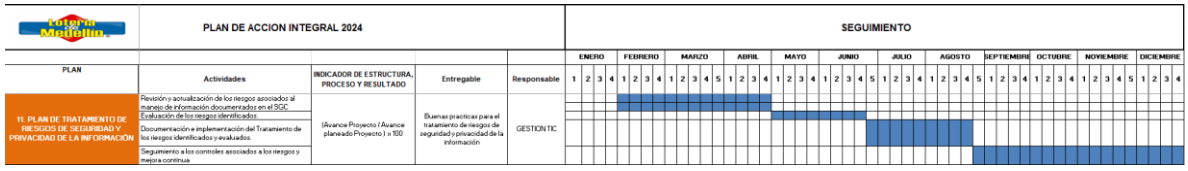
DESARROLLO DEL PLAN

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 debenser 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.

CRONORAMA DE ACTIVIDADES



MEDICIÓN

% 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 2024.

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)