TABLA DE CONTENIDO

INTRODUCCIÓN 1
1. OBJETIVO 2
2. ALCANCE 3
3. RESPONSABLES. 3
4. DEFINICIONES 3
5. MARCO NORMATIVO 6
6. DESARROLLO 6
7. DOCUMENTOS Y REGISTROS RELACIONADOS 8
8 CONTROL DE CAMBIOS 9
9. ANEXOS 9

ELABORÓ	REVISÓ	APROBÓ
Nombre: Elmer Francisco Castro Cargo: Profesional Universitario	Nombre: Luz Stella Manrique Muñoz Cargo: Subgerente Administrativo y Financiero	Nombre: Wilintong Ortiz Arias Cargo: Gerente

INTRODUCCIÓN

La Política de Gobierno Digital, definida por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, tiene como propósito promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) para consolidar un Estado eficiente, transparente e innovador, generando valor público en un entorno de confianza digital.

En este contexto, el habilitador de Seguridad y Privacidad de la Información establece la obligación de implementar controles de seguridad sobre los procesos, trámites, servicios, sistemas de información, infraestructura tecnológica y activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El Modelo de Seguridad y Privacidad de la Información (MSPI) define la gestión del riesgo como el eje central para la protección de la información institucional, permitiendo identificar, analizar, evaluar y tratar los riesgos que puedan afectar los activos de información, generando confianza a las partes interesadas.

En concordancia con el Modelo Integrado de Planeación y Gestión – MIPG, el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los riesgos identificados que puedan afectar uno o varios procesos de la Lotería del Meta, constituyéndose en un instrumento fundamental para la toma de decisiones y la mejora continua del Subsistema de Gestión de Seguridad de la Información.

1. OBJETIVO

1.1. OBJETIVO GENERAL

Establecer un marco de acción para el tratamiento de los riesgos de seguridad y privacidad de la información asociados a los activos de información de la Lotería del Meta, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, apoyando el cumplimiento de los objetivos estratégicos de la Entidad.

1.2. OBJETIVOS ESPECIFICOS

- Identificar y priorizar los riesgos de seguridad y privacidad de la información que puedan afectar los procesos institucionales.
- Definir acciones y controles para mitigar, reducir, aceptar o transferir los riesgos identificados.
- Establecer roles y responsabilidades frente al tratamiento de los riesgos de seguridad de la información.

- Fortalecer los controles existentes mediante acciones de mejora continua.
- Facilitar el seguimiento, monitoreo y evaluación del tratamiento de los riesgos implementados.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica a todos los procesos, dependencias, sistemas de información, infraestructura tecnológica, servicios digitales y activos de información de la Lotería del Meta.

El plan prioriza los riesgos clasificados en niveles Moderado, Alto y Extremo, de acuerdo con la metodología de gestión del riesgo definida por el Ministerio TIC y la Entidad. Los riesgos clasificados en niveles bajos podrán ser aceptados, previa aprobación de la alta dirección, y estarán sujetos a monitoreo periódico.

3. RESPONSABLES.

El presente plan es de obligatorio cumplimiento para:

- Funcionarios de planta
- Contratistas
- Proveedores de servicios tecnológicos
- Usuarios con acceso a la información institucional

Los propietarios de los activos de información, custodios y usuarios son responsables de la correcta aplicación de los controles definidos y del reporte oportuno de eventos o incidentes de seguridad de la información.

4. DEFINICIONES

Se adoptan las definiciones establecidas en las normas ISO/IEC 27001, ISO 73 y en el Modelo de Seguridad y Privacidad de la Información (MSPI), relacionadas con la gestión del riesgo, activos de información, amenazas, vulnerabilidades, controles, incidentes y tratamiento de riesgos.

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva: Medida de tipo proactivo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto [Fuente: Guía ISO 73: 2009].

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. La aceptación del riesgo puede ocurrir sin tratamiento de riesgo o durante el proceso de tratamiento de riesgo. Los riesgos aceptados están sujetos a monitoreo y revisión.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. [Fuente: Guía ISO 73: 2009] El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Ataque: Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Continuidad de la seguridad de la información: Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.

Control: Medida por la que se modifica el riesgo. [Fuente: ISO Guide 73:2009] Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o

supuesto. El término salvaguardado contramedida son utilizados frecuentemente como sinónimos de control.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos. [Fuente: ISO Guide 73:2009]

Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos [Fuente: Guía ISO 73:2009]. La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.

Impacto: El coste para la empresa de un incidente -de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.-.

Indicador: Medida que proporciona una estimación o evaluación.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO NORMATIVO

La actualización del plan estratégico de seguridad y privacidad de la información se define teniendo en cuenta el siguiente marco normativo:

CONPES 3995 de 2020: "POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL".

Decreto 1008 de 2018: "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"

Decreto 415 de 2016: (Lineamientos fortalecimiento institucional en TIC), Se adiciona el decreto único reglamentario del sector de la función pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones; Arts. 2.2.35.5; 2.2.35.6

Decreto 1078 de 2015:, "Decreto Único Reglamentario del sector TIC. En particular las normas referentes a la Estrategia de Gobierno en Línea."

Ley 1712 de 2014: (Acceso a la información pública y Uso de las TIC), "Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente."

Ley 1581 de 2012(Habeas data): "Se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la ley 1266 de 2008, excepto los principios."

NORMA TÉCNICA COLOMBIANA NTC - ISO/IEC 27001: "Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa"

6. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS

El tratamiento de los riesgos de seguridad y privacidad de la información se desarrolla conforme a la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas y al MSPI, priorizando la implementación de controles técnicos, administrativos y organizacionales.

Las principales acciones de tratamiento incluyen:

- Implementación y fortalecimiento de controles de seguridad de la información.
- Seguimiento a la operación y efectividad de los controles implementados.
- Evaluación periódica de los riesgos residuales.
- Actualización del plan de tratamiento de riesgos conforme a cambios tecnológicos, organizacionales o normativos.

En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de Seguridad y Privacidad de la Información:

Actividad	**Responsable**	**1 semestre 2026**						**2 semestre 2026**					
		E	**F**	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**
Realizar la Adquisición e implementación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las áreas y oficinas de la Lotería del Meta		X	X	X	X	X	X	X	X	X	X	X
Realizar los procesos requeridos para el seguimiento a la operación de los controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Todas las áreas y oficinas de la Lotería del Meta		X	X	X	X	X	X	X	X	X	X	X
Realizar el seguimiento a las	Área de												

actividades de identificación y operación de controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información bajo la responsabilidad de cada dependencia a nivel central.	Sistemas			X			X			X			X	

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, al deseo de riesgo institucional y a las orientaciones de la gerencia, en cuanto al deseo de riesgo institucionales que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.

Para el desarrollo de las actividades, el área de sistemas contará con un equipo humano dispuesto para adelantar actividades de sensibilización, capacitación y atención de inquietudes a las oficinas de la Lotería del Meta a través de cronogramas definidos.

El área de sistemas ha establecido unos tiempos en los cuales se brindará y apoyará el seguimiento al desarrollo de los planes de seguridad y privacidad de la información que las dependencias presenten y así tratar las actividades pertinentes a los procesos relacionados al diligenciamiento de los planes de seguridad y privacidad de la información.

7. SEGUIMIENTO, MONITOREO Y MEJORA CONTINUA

El área de Sistemas realizará el seguimiento periódico al cumplimiento del Plan de Tratamiento de Riesgos, apoyando a las dependencias en la ejecución de las acciones definidas y verificando la efectividad de los controles implementados.

El seguimiento estará sujeto a la disponibilidad de recursos humanos, técnicos y financieros, a las probabilidades de riesgo institucional y a las directrices de la alta dirección, promoviendo la mejora continua del Subsistema de Gestión de Seguridad de la Información.

8. DOCUMENTOS Y REGISTROS RELACIONADOS

DOCUMENTOS Y REGISTROS RELACIONADOS	
Código	**Nombre**
N/a	N/a

9 CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión	**Fecha**	**Descripción y razón del cambio**
1	05/06/2024	Primera versión y creación del documento
2	2026	Actualización y alineación con MSPI y Gobierno Digita

9. ANEXOS

N.A.