

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

LOTERIA DEL TOLIMA – 2026

Tabla de Contenido	
DEFINICIONES	3
RIESGO DE SEGURIDAD DE LA INFORMACIÓN:	3
OBJETIVOS	4
OBJETIVOS ESPECÍFICOS	4
ALCANCE	4
MARCO NORMATIVO	4
MARCO TEÓRICO	5
ETAPAS PARA LA GESTIÓN DE RIESGOS	7
Etapas de Identificación	7
Etapas de Medición	7
Etapas de control	7
Etapas de monitoreo	8
CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	8
TRATAMIENTO Y FINALIDADES	8

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Lotería del Tolima E.I.C.E. permite definir y aplicar los controles necesarios para mitigar la materialización de riesgos dentro de la entidad. Este plan se complementa con una adecuada documentación, socialización y la adopción de buenas prácticas, con el objetivo de fortalecer la protección de la entidad frente a dichos riesgos. Asimismo, incorpora controles específicos en los procesos de la organización para garantizar su eficacia y alineación con los objetivos institucionales.

DEFINICIONES

RIESGO: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN:

Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

RIESGO POSITIVO: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

SEGURIDAD DE LA INFORMACIÓN: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos

preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano

INFORMACIÓN PÚBLICA RESERVADA: Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

INFORMACIÓN PÚBLICA CLASIFICADA: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.



NO CLASIFICADA: Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PÚBLICA RESERVADA.

CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos.

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

OBJETIVOS

OBJETIVO GENERAL

Velar por los activos de información de la entidad durante el año 2025 frente a acciones o eventos que puedan comprometer su disponibilidad, integridad o confidencialidad.

OBJETIVOS ESPECÍFICOS

- Identificar los riesgos asociados al tratamiento de la información en la Lotería del Tolima
- Calcular el nivel de riesgo al que está expuesta la información dentro de la entidad
- Definir el plan de tratamiento de riesgos que se va a llevar a cabo en la entidad
- Realizar seguimiento y control al plan diseñado para el tratamiento de los riesgos
- Promover el uso de mejores prácticas de seguridad de la información, que impidan el acceso a la información por terceros no autorizados
- Definir tratamiento y finalidades

ALCANCE

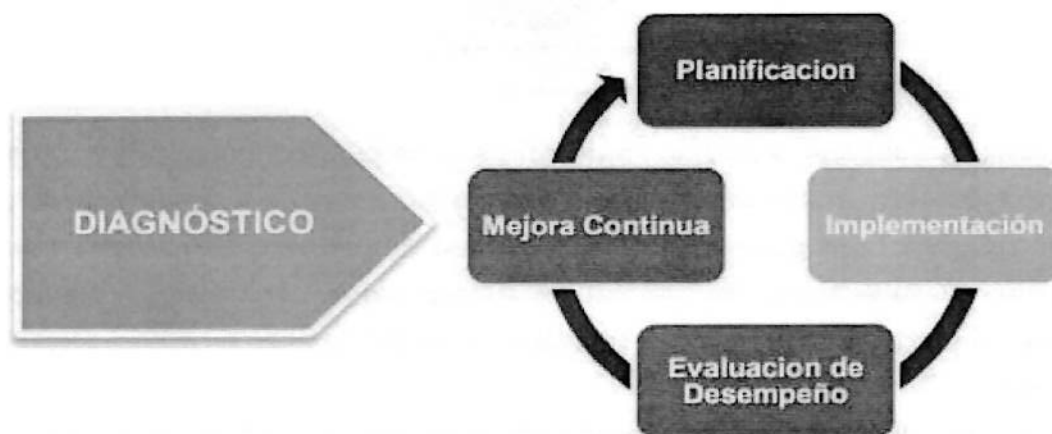
Se define el alcance del presente plan de tratamiento de riesgos, para los procesos misionales y de apoyo de la Lotería del Tolima.

MARCO NORMATIVO

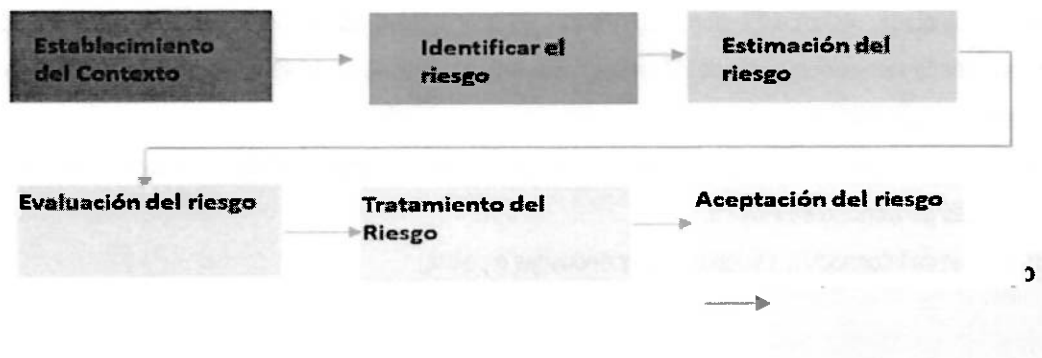
- Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y de las comunicaciones
- 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.

Implementar la seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información, en cualquiera de sus estados, ante cualquier amenaza o brecha que pueda atentar contra los principios fundamentales de confidencialidad, integridad y disponibilidad; establecer medidas de control de seguridad de la información, le permite a la entidad gestionar y mitigar los riesgos e impactos a las que se pueda ver expuesta. La técnica de análisis de riesgo para activos de información permite a la Lotería del Tolima estar preparado ante cualquier amenaza que pueda vulnerar o afectar la información, cabe resaltar que todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos.

A continuación, se presenta el ciclo de operación del modelo de seguridad y privacidad de la información y las actividades generales para la implementación del plan.



Ciclo de operación del Modelo de Seguridad y Privacidad de la Información Fuente: MINTIC



La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA):



Uno de los objetivos del modelo de seguridad y privacidad de la Información es el de garantizar un adecuado manejo de la información pública en poder de las entidades destinatarias, la cual es uno de los activos más valiosos para la toma de decisiones, el modelo propende por un doble enfoque a saber: a nivel de seguridad marcando un derrotero para que las entidades destinatarias construyan unas políticas de seguridad sobre la información a fin de salvaguardar la misma a nivel físico y lógico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad.

En esa línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la administración como el acceso a la información pública cuando esta no se encuentre sometida a reserva. Para ello se requiere dotar al modelo de seguridad de la información de un componente específico relacionado con la privacidad. Para que los servidores públicos entiendan mejor el concepto de privacidad, hay que tener claro que diferentes procesos relacionados con la recolección y uso de información son susceptibles de ser objeto de implementación de medidas de privacidad, como puede ser:

- El Desarrollo de políticas que impliquen la necesidad de recolectar y usar información personal, como por ejemplo políticas de atención de PQR'S.
- La Transferencia de información a terceros (otras entidades o países).

ETAPAS PARA LA GESTIÓN DE RIESGOS

Para la gestión del riesgo en la lotería del Tolima se establecen las siguientes etapas:

Etapas de Identificación

La lotería del Tolima realiza la identificación de sus riesgos con un enfoque basado en procesos, donde toma como fundamento el objetivo del mismo para la definición de los riesgos. La identificación del riesgo es responsabilidad del líder del proceso, así mismo, en esta etapa se define el riesgo, sus causas, fuentes, procesos y activos de información asociados, así como el responsable de su gestión.

Etapas de Medición

La entidad establece las métricas para la medición de la probabilidad e impacto de los riesgos identificados por el Líder de Proceso. En esta etapa se establecen el impacto legal, reputacional y operativo el cual incluye los aspectos asociados a la seguridad y privacidad de la información (disponibilidad, integridad y confidencialidad), los cuales se consideran relevantes para la continuidad y credibilidad de la entidad.

PROBABILIDAD	IMPACTO				
	INSIGNIFICANTE 1	ME-NOR 2	MO-DE-RAD O 3	MA-YOR 4	CATASTRO-FICO 5
E - RARO - 1	B	B	M	A	A
D - IMPROBABLE - 2	B	B	M	A	E
C - POSIBLE - 3	B	M	A	E	E
B - PROBABLE - 4	M	A	A	E	E
A - CASI CERTEZA - 5	A	A	E	E	E

ZONA DE RIESGO BAJA

ZONA DE RIESGO MODERADA

ZONA DE RIESGO ALTA

ZONA DE RIESGO EXTREMO

Etapas de control

Esta etapa para la gestión de los riesgos operativos es responsabilidad del Líder del Proceso, ya que debe definir las acciones concretas para mitigar el riesgo, y custodiar los activos a su cargo.

Los controles deben estar documentados preferiblemente dentro de los procedimientos con el objeto de contar con la trazabilidad necesaria de su aplicación, así como la exigibilidad de su uso por parte los encargados de su ejecución.

La oficina de control interno mediante las auditorias que pueden identificar los riesgos existentes y las acciones de mejora por el líder del proceso.

Etapa de monitoreo

La lotería del Tolima E.I.C.E cuenta con diversas herramientas de monitoreo de los riesgos, como primer filtro, se encuentra el Líder de Proceso, debe supervisar que los controles de su proceso se estén ejecutando a través de la definición de indicadores, revisiones aleatorias u otros mecanismos que considere pertinentes, revisión por parte de la dirección.

Así mismo, La auditoría interna se debe realizar periódicamente y cuyos resultados son insumo para que el Líder del Proceso fortalezca la gestión de los riesgos.

El líder del proceso debe establecer un documento denominado Matriz de Riesgos el cual se usa para identificar, evaluar y priorizar los riesgos que pueden afectar a una organización. Su objetivo es ayudar a tomar decisiones informadas para hacer frente a los riesgos identificados en la entidad.

CRONOGRAMA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

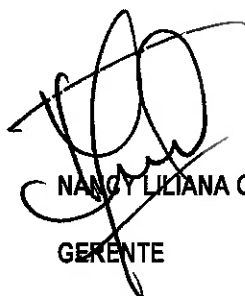
N°	Actividad	Riesgo que trata	Responsable	Inicio	Fin	Frecuencia	Producto Evidencia
1	Identificación y actualización de activos de información	Pérdida o uso indebido de información	Oficina de Sistemas	Enero	Enero	Anual	Inventario de activos actualizado
2	Identificación y análisis de riesgos de seguridad	Accesos no autorizados	Oficina de Sistemas	Febrero	Febrero	Anual	Matriz de riesgos
3	Definición del plan de tratamiento de riesgos	Riesgos no mitigados	Oficina de Sistemas	Febrero	Marzo	Anual	Plan de tratamiento aprobado
4	Implementación de controles de acceso a sistemas de información	Acceso no autorizado	Oficina de Sistemas	Marzo	Abril	Permanente	Configuración de usuarios y perfiles
5	Fortalecimiento de copias de seguridad (backups)	Pérdida de información crítica	Oficina de Sistemas	Marzo	Abril	Permanente	Registros de backups
6	Actualización de antivirus, parches y software	Malware y vulnerabilidades	Oficina de Sistemas	Mayo	Mayo	Anual	Reportes de actualización
7	Capacitación en seguridad y privacidad de la información	Errores humanos	Talento Humano / Sistemas	Junio	Junio	Semestral	Listas de asistencia

TRATAMIENTO Y FINALIDADES

La Lotería del Tolima, lleva a cabo el tratamiento de datos personales, a todos los que están relacionados con el desarrollo de su actividad comercial e industrial, cumpliendo con lo establecido por la Constitución y la Ley.

Los datos personales serán tratados de acuerdo con los grupos de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se presenta en la siguiente tabla:

Grupo de Interés	Finalidad	Dependencia Responsable
Autorización para grabación y difusión de contenido audiovisual	Gestionar la respectiva autorización del uso de imagen y/o audio para hacer difusión, promoción de campañas establecidas por la Entidad.	Unidad Operativa y Comercial
Promoción de marca propia y externa	Gestionar de manera oficial los términos y condiciones en que se hará uso de la marca y/o productos que utilizará la Lotería del Tolima o de otra entidad.	Unidad Operativa y Comercial
Consultas Restrictivas	Cuando existe vinculación de funcionarios, contratistas o distribuidores a la Entidad se debe realizar el filtro por las listas restrictivas de la unidad de información y análisis financiero (UIAF)	Unidad Operativa y Comercial Unidad Administrativa
Imagen Redes Sociales	Gestionar la respectiva autorización del uso de imagen para hacer difusión en redes sociales de terceros	Unidad Operativa y Comercial
Imagen Billetería	Gestionar la respectiva autorización del uso de imagen de terceros en la billetería	Unidad Operativa y Comercial



NANCY LILIANA CRISTANCHO SANTOS
GERENTE

Elaboro: Nilly Rocio Yate Guzmán  Técnico de sistemas
Reviso: Yineith Paola Villanueva Molina  Profesional especializada de la unidad administrativa

