LOTERÍA DEL TOLIMA

APUÉSTELE A SUS SUEÑOS

SC-CER804982

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

EMPRESA INDUSTRIAL Y COMERCIAL DEL ESTADO LOTERIA DEL TOLIMA E.I.C.E

ENERO 2023

Carrera 2 No. 11 – 59 Piso 2 Ibagué - Tolima
Tel. (608) 2631883 – (608) 2611023
Línea de atención al Cliente 018000 942542
"El Tolima nos Une"

www.loteriadeltolima.com
@loteriatolima *@loteriatolima* *@loteria_tolima*

1. OBJETIVO GENERAL:

Elaborar el plan de tratamiento de riesgos de Seguridad y privacidad de la Información de la lotería del Tolima E.I.C.E., que permita definir y aplicar los controles necesarios que mitiguen la materialización del riesgo dentro de la entidad.

1.1 OBJETIVOS ESPECIFICOS

- 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.

2. ALCANCE

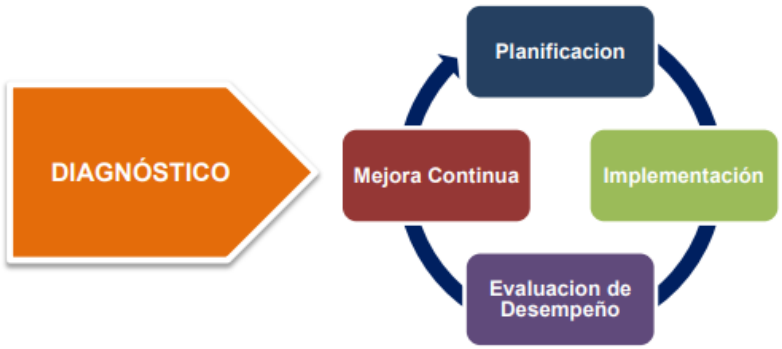
Se define el alcance del presente plan de tratamiento de riesgos, para los procesos misionales y de apoyo de la Lotería del Tolima.

3. MARCO TEÓRICO

Implementar la seguridad de la Información en las empresas tiene como fundamental 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 qué 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 se 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

Estructura general de la metodología de riesgos

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):

- Establecer contexto
- Evaluación del riesgo
- Tratamiento del Riesgo

Implementar procesos de mejora continua

Implementar plan de tratamiento de riesgos de seguridad y privacidad de la información

Supervisión y revisión del plan y del cumplimiento de las actividades propuestas.

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:

- La Implementación de un sistema de información que tenga la posibilidad de recolectar datos personales, tal como un sistema de seguridad a través de video vigilancia que capture imágenes, datos biométricos, etc.
- El Diseño y ejecución de un sistema de gestión documental.
- 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).

4. ETAPAS PARA LA GESTIÓN DE RIESGOS

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

4.1 Etapa 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 de la primera línea de defensa, es decir del dueño 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.

4.2 Etapa 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	MENOR 2	MODERADO 3	MAYOR 4	CATASTROFICO 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

B	ZONA DE RIESGO BAJA
M	ZONA DE RIESGO MODERADA
A	ZONA DE RIESGO ALTA
E	ZONA DE RIESGO EXTREMO

4.3 Etapa de control

Esta etapa para la gestión de los riesgos operativos es responsabilidad del Líder del Proceso, ya que debe definir las acciones concretas a través de las cuales gestionará el riesgo y/o custodiará 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 de los encargados de su ejecución.

4.4 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.

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.

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

Actividad	Mes											
	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1. Etapa de Identificación		01-01 / 31-05										
2. Etapa de Medición						01-06 / 31-10						
3. Etapa de control						01-06 / 31-10						
4. Etapa de monitoreo											01-11 / 15-12	

6. TÉRMINOS Y 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 Publica 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 PUBLICA 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.

Aprobado COMITÉ INSTITUCIONAL DE GESTION, mediante Acta No. 001 del 24 de enero de 2023