EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN

ÁREA DE SISTEMAS

BOGOTA, 2021

1. INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital. - Versión 4 emitida por el DAFP.

2. DEFINICIONES:

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 que 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.

3. OBJETIVOS

Definir y aplicr los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la Lotería de Bogotá pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

4. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016): se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información de la Lotería de Bogotá.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por la Lotería de Bogotá, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

5. MARCO REFERENCIAL

POLÍTICA DE ADMINISTRACION DE RIESGOS

La Lotería de Bogotá, en coherencia con su Modelo Integrado de Planeación y Gestión en cada uno de sus trece (13) procesos, así como los lineamientos de la Guía para la administración del riesgo de la Función Pública 2018, la cual integra los diferentes riesgos, se compromete a monitorear y controlar los riesgos que puedan impedir el cumplimiento de las metas y objetivos organizacionales, desde un análisis del contexto estratégico y de los factores internos y externos de la Entidad, garantizando la efectividad de los procesos en el manejo adecuado de los riesgos y con la participación activa y compromiso de todos los servidores de cada uno de los Procesos.

La responsabilidad de los riesgos se encuentra relacionada en la Política de Administración de riesgo de la Lotería de Bogotá, la cual está estructurada por líneas de defensa.

6. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera.

GESTION	ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMADAS	
				Fecha Inicial	Fecha Final
Gestión de Riesgos	Actualización de lineamientos de riesgos de Seguridad de la Información.	Actualización de la política y metodología de gestión de riesgos	Planeación - Sistemas	1/02/2021	30/06/2021
	Sensibilización	Socialización de la política y metodología de Gestión de Riesgos de Seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Sistemas	1/07/2021	31/07/2021
	Identificación, Análisis y Evaluación	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Sistemas	1/07/2021	31/07/2021
	Aceptación y Aprobación	Aceptación, aprobación Riesgos identificados y planes de tratamiento.	CIGD	1/08/2021	31/08/2021
	Publicación	Publicación Matriz de riesgos	Sistemas	Una vez sea aprobado	
	Monitero a los riesgos de SPI	Diligenciamiento del instrumento	Sistemas	De acuerdo a registrado en el instrumento.	
	Evaluación del riesgo	Evaluación de riesgos residuales	Planeación		
	Seguimiento y Revisión	Generación, presentación y reporte de indicadores	Planeación	Trimestral	

7. DESARROLLO METODOLÓGICO

Fase 1: Análisis de la información

En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.

- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

Fase 3: Análisis de los proyectos

- - Definición de los controles relacionados con cada medida.
- - Validar los riesgos mitigados por cada medida.
- - Análisis de la aplicabilidad de las medidas.
- - Priorización de las medidas.

Fase 4: Definición del organigrama de responsabilidad

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por la Lotería de Bogotá, teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones de la Lotería de Bogotá, en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte de la Lotería de Bogotá,
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

Fase 5: Ciclo de vida del tratamiento de riesgos

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

8. OPORTUNIDAD DE MEJORA

La Lotería de Bogotá, no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

9. RECURSOS

La Lotería de Bogotá, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos.

RECURSOS	VARIABLE
Humanos	El Área de Sistemas es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

10. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información, depende de la necesidad identificada frente a la Seguridad y Privacidad de la Información, con el liderazgo de a la Alta Dirección, frente a la consecución de los recursos.

11. MEDICIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión o desempeño que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que sirven como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la información.

12. MEDICIÓN

La medición se realiza con un indicador de gestión o desempeño, que está orientado principalmente a determinar el porcentaje de implementación y/o ejecución de los controles definidos en el tratamiento de riesgos de seguridad y privacidad de la información.