PLAN DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ÁREA DE SISTEMAS

BOGOTÁ, 2021

1. INTRODUCCIÓN

El presente documento contiene los lineamientos del Modelo de Seguridad y Privacidad de la MSPI versión 3.0.2 definido por MINTIC, el cual orienta a las entidades a la preservación de la confidencialidad, integridad, disponibilidad de la información y permite fijar los criterios para proteger la privacidad de la información, los datos, así como de los procesos y las personas vinculadas con dicha información

Para la elaboración de este documento, se toma como referencia además de los lineamientos de MINTIC en el MSPI y sus correspondientes guías de apoyo, la norma ISO 27001:2013 y el anexo A.

Las políticas de seguridad de la información incluidas en este documento constituyen una parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital y se convierten en la base para la implementación de los controles, procedimientos definidos por las normas anteriormente mencionadas.

Es responsabilidad de todas las partes interesadas de la Lotería de Bogotá, velar por que no se realicen actividades que contradigan la esencia de este documento con el fin de preservar la confidencialidad, integridad y disponibilidad de la información que aquí se maneja.

2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Establecer las actividades tendientes a fortalecer la seguridad y privacidad de la información de la Lotería de Bogotá, mediante la planeación de acciones contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013 y la Política de Seguridad Digital.

3. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

1.Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.

2.Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación de los servicios.

3.Mitigar el impacto de los incidentes de Seguridad y Privacidad de la Información y de Seguridad Digital, de forma efectiva, eficaz y eficiente.
4.Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información de la Lotería de Bogotá.

5.Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.

6.Generar un cambio organizacional a través de la conciencia y apropiación de la Seguridad y Privacidad de la Información y la Seguridad Digital.

7.Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.

8.Definir, operar, mantener el Plan de Continuidad de la Operación de los servicios del la Lotería de Bogotá.

4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El plan de seguridad y privacidad de la información aplica a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la Lotería de Bogotá, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por la Lotería de Bogotá, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

5. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de Seguridad de la Información son asumidas por el Comité del Integrado de Gestión y Desempeño (CIGD) mediante Resolución No. 68 de 2019.

6. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GESTION	ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMADAS	
				Fecha Inicial	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de activos de información	Recursos Físicos	1/03/2021	30/06/2021
		Socializar la guía de activos de Información		1/07/2021	31/07/2021
	Levantamiento Activos de Información	Validar activos de información en el instrumento levantado en la vigencia anterior	Todas las dependencias	30/08/2021	
		Identificar nuevos activos de información en cada dependencia	Todas las dependencias		
		Actualizar los activos de información	Recursos Físicos	30/09/2021	
		Aprobar los activos de información	CIGYD	Cada vez que se modifiquen o actualicen.	
	Publicación de Activos de Información	Publicar los activos de información	Recursos Físicos – Sistemas	Cada vez que se modifiquen o actualicen.	
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	
	Monitoreo 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	

GESTION	ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMADAS	
				Fecha Inicial	Fecha Final
Gestión de Incidentes de Seguridad de la Información	Definir incidentes de seguridad de la información	Definir procedimiento de incidentes de seguridad de la información	Sistemas	1/05/2021	31/05/2021
	Socializar y Publicar el procedimiento de incidentes de seguridad de la información	Socializar y publicar el procedimiento de incidentes de seguridad de la información	Sistemas	1/06/2021	30/06/2021
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	Sistemas	Cada vez que se requiera.	
	CSIRT -	Revisar de manera semanal la página web de CSIRT, para determinar eventos de vulnerabilidad que puedan afectar la seguridad de la información de la entidad.	Sistemas	Semanal	
		Socializar los boletines informativos de seguridad, que resulten de la revisión anterior e Integrar con CSIRT de Gobierno	Sistemas	Cada vez que se requiera.	
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación y aprobación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear y aprobar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Secretaria General – Sistemas - CIGYD	1/06/2021	30/06/2021
	Publicación	Publicación de Matriz de Requisitos Legales de Seguridad de la Información, de acuerdo a la estructura del normograma.	Sistemas	1/07/2021	15/07/2021
Planeación	Revisión y aprobación Manual Políticas de Seguridad de la Información	Aprobar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información.	Sistemas - CIGYD	1/02/2021	31/05/2021
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Sistemas	1/02/2021	31/03/2021
		Generar el plan de mejora de acuerdo a los resultados del autodiagnóstico del MSPI	Sistemas	1/04/2021	30/04/2021
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	Sistemas	1/04/2021	30/04/2021
		Monitorear y hacer seguimiento el avance de implementación del Plan de Seguridad Digital en la Entidad	Sistemas	De acuerdo a registrado en el instrumento.	
		Socialización con los servidores de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Sistemas	Anual	

GESTION	ACTIVIDADES	TAREAS	RESPONSABLE	FECHAS PROGRAMADAS	
				Fecha Inicial	Fecha Final
Vulnerabilidades	Definir lineamientos para ejecutar análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Definir los lineamientos, estudios previos, pliego de condiciones para la realización de análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Sistemas	1/07/2021	31/07/2021
	Contratar análisis GAP, análisis de vulnerabilidades y Éthical Hacking	Realizar el contrato para realizar análisis GAP, análisis de vulnerabilidades y Éthical Hacking teniendo en cuenta el alcance y metodología	Secretaria General - Sistemas	31/07/2021	31/08/2021
	Ejecución del contrato	Ejecución del contrato de análisis GAP, análisis de vulnerabilidades y Éthical Hacking de acuerdo a **las obligaciones del mismos.**	Contratista - Supervisor	1/09/2021	31/12/2021
	Iniciar la ejecución del plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis GAP, análisis de vulnerabilidades y Ethical Hacking	Sistemas	Sujeto a la ejecución del contrato (Plan de remediación entregada por el contratista)	
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Secretaría General - Sistemas	Primer trimestre	
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Todas las dependencias	30/04/2021	
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Sistemas	31/05/2021	
	Revisar, actualizar y publicar	Revisar y actualizar la política de protección de datos personales. Publicar en página web de la entidad y en la SIC.	Sistemas - Planeación - Talento Humano - Atención al Cliente.	30/06/2021	

7. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000.Por medio de la cual se expide la Ley General de Archivos.
- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas

- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1221 del 2008.Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1341 de 2009.Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones -TIC-Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- Ley 1474 de 2011.Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1581 de 2012.Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014.Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- Ley 1952de 2019.Por medio de la cual se expide el código general disciplinario
- Ley 1955 de 2019.por el cual se expide el Plan Nacional de Desarrollo 2018-2022. “Pacto por Colombia, Pacto por la Equidad”.
- Ley 1978 de 2019. Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- Decreto 0884 del 2012.Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014.Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015.Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015.Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.