Objetivo:

Establecer las actividades y responsabilidades para indicar como responde la Lotería de Bogotá en caso de presentarse algún incidente que afecte la Disponibilidad, Integridad o confidencialidad de la información.

Alcance:

Inicia con el reporte de un posible incidente de seguridad de la información, atención, tratamiento y respuesta del mismo y finaliza con la solución e identificación de lecciones aprendidas.

Definiciones:

1 **CONFIDENCIALIDAD:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [ISO/IEC 27000:2017].

2 **DISPONIBILIDAD:** Propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000:2018]

3 **INTEGRIDAD:** Propiedad de exactitud y completitud. [ISO/IEC 27000:2017].

4 **INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2009]

5 **NO REPUDIO:** Con la expresión "no repudio" se hace referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o

6 **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC 27000:2009]

7 **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

8 **SEGURIDAD DIGITAL:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Políticas de Operación:

1 La gestión de incidentes tiene un ciclo de prevención, respuesta, monitoreo, evaluación y aprendizaje el cual genera mejora en la Lotería de Bogotá y evita la reincidencia de los incidentes en seguridad de la información.

2 La correcta gestión de incidentes trae consigo beneficios tangibles como económicos y legales, así como beneficios intangibles tales como la protección de la imagen y la confianza de clientes y terceros en la Lotería de Bogotá.

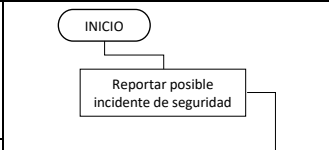
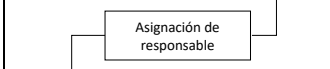
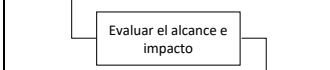
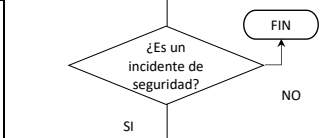
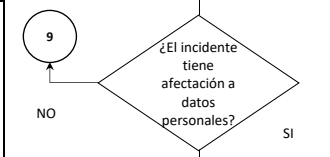
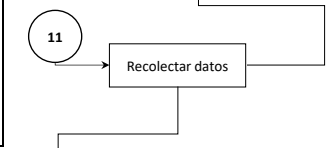
3 La gestión de incidentes comprende las siguientes fases:

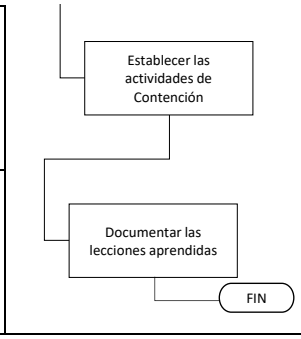
- Planeación y preparación: Se debe de estar preparado para responder antes que el incidente ocurra. Por tanto se deben establecer niveles de protección físicos y lógicos que sean adecuados para la salvaguarda de la infraestructura tecnológica y la información de la organización.
- Identificación del incidente: Se debe determinar si el incidente realmente existe, así como obtener la mayor cantidad de información disponible como insumo para su tratamiento adecuado.
-Manejo del incidente: Se debe responder al incidente de manera que se ejecuten las actividades de contención ante el incidente, erradicación del mismo y recolección y cuidado de evidencias para propósitos de investigación de las causas y/o legales.

Documentos de soporte:

CÓDIGO	NOMBRE	ENTIDAD
N/A		Lotería de Bogotá

Actividades

#	Actividad	Descripción: Cómo, Políticas, Criterios de aceptación o rechazo, Instructivos	Registro	Responsable
1		Reportar a través de la herramienta de soporte e TI o por correo electrónico al área de sistemas, indicando: - Identificación y contacto de quien reporta. - Descripción detallada del incidente.	Herramienta de Mesa de Servicios de TI	Solicitante
2		Asignar una persona responsable para evaluar el incidente.	Mesa de servicio Nivel 0	Área de sistemas Oficina de Gestión Tecnológica e Innovación e Innovación
3		Evaluar el alcance e impacto del problema determinando los límites del incidente. Identifique el impacto del ataque en términos de: - personas. - hardware. - software. - datos. - documentación (información física) - comunicaciones.	Mesa de servicio Nivel 0	Área de sistemas Oficina de Gestión Tecnológica e Innovación e Innovación
4		**¿Es un incidente de seguridad de la información?** **NO**: Documentar en la herramienta el análisis realizado y FIN. **SI:** Continua en la pregunta 5	Herramienta de Mesa de Servicios de TI	Área de sistemas Oficina de Gestión Tecnológica e Innovación e Innovación
5		**¿El incidente tiene afectación a datos personales?** **NO:** Continua en la pregunta ¿Se autoriza el cambio? **SI:** Continua en la pregunta 6	Herramienta de Mesa de Servicios de TI	Área de sistemas Oficina de Gestión Tecnológica e Innovación e Innovación
6		Recolectar datos preliminares del incidente revisando los logs centralizados. y busque anormalidades en los sistemas. Realice entrevistas tomando nota de cada paso, identificando quién hizo qué, cuándo, cómo y por qué. Estas notas deben ser cronológicas, indicando el tiempo de cada entrada.	Acta, reunión, informe técnico, logs, informes de herramientas.	Área de sistemas Oficina de Gestión Tecnológica e Innovación e Innovación

7		Establecer las actividades de Contención que limiten el alcance e impacto del ataque.	Acta, reunión, informe técnico	Área de sistemas Oficina de Gestión Tecnológica e Innovación e Innovación
8		Documentar las lecciones aprendidas como medida de prevención para minimizar la materialización de riesgos que generan incidentes de seguridad de la información.	Herramienta de mesa de servicio de TI, correo, oficio	Área de sistemas Oficina de Gestión Tecnológica e Innovación e Innovación

Relación de registros

CÓDIGO TRD	NOMBRE	FÍSICO	DIGITAL
N/A	Acta de control	X	X
N/A	Acta de seguimiento	X	X
N/A	Informes	X	X

Control de cambios

FECHA	DESCRIPCIÓN Y JUSTIFICACIÓN DEL CAMBIO	VERSIÓN
	Creación	1
12/10/2023	Se actualiza en el marco de la certificación en norma ISO37001	2

Control de revisión y aprobación

Elaboración	Revisión	Aprobación
Yolanda Patricia Gallego Galvis **Profesional Especializado**	**Oscar Fabian Melo Vargas** **Jefe Oficina Asesora de Planeación**	Comité Institucional de Gestión y Desempeño