



La que más billete da

**MANUAL DE GESTIÓN DE LA
SEGURIDAD DE LA INFORMACIÓN
(SGSI)**

**LOTERÍA DE BOGOTÁ
OFICINA DE GESTIÓN
TECNOLÓGICA E INNOVACIÓN**

Abril 21 de 2025

TABLA DE CONTENIDO

INTRODUCCIÓN	3
1. ALCANCE	3
2. DEFINICIONES	4
3. REFERENCIAS NORMATIVA	6
4. CONTEXTO DE LA ENTIDAD	9
4.1 Comprensión de las necesidades y expectativas de los clientes y las partes interesadas... 11	
5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	12
5.1 Documentación del SGSI.....	12
5.2 Política general del SGSI.....	13
5.3 Objetivo general.....	14
5.4 Objetivos específicos	14
5.5 Políticas específicas y complementarias de seguridad y privacidad de la información.....	15
5.6 Compromiso y liderazgo de la Dirección.....	15
6. ROLES Y RESPONSABLES.....	17
6.1 Identificación de los responsables	17
6.2 Equipo de gestión al interior de la Lotería de Bogotá.....	18
6.3 Responsable de la Seguridad de la Información o quien haga sus veces para la Lotería de Bogotá.....	18
6.4 Comité de Gestión y Desempeño de la Lotería de Bogotá.....	20
6.5 Oficina asesora Jurídica de la Lotería de Bogotá.....	21
6.6 Gestión del Talento Humano de la Lotería de Bogotá.....	21
6.7 Oficina de Control Interno	22
6.8 Separación de deberes.....	22
6.9 Contacto con autoridades y grupos de interés	22
6.10 Equipo técnico del SGSI	23
6.11 Jefe Oficina de Gestión Tecnológica e Innovación:.....	24
6.12 Oficial de seguridad de la información o quien haga sus veces.....	24
6.13 Profesional infraestructura TI.....	25
6.14 Profesional servicios tecnológicos o quien haga sus veces. (Web Master, profesional de apoyo de la Oficina)	26
6.15 Profesional responsable de los sistemas de información (Web Master, profesional de apoyo de la Oficina).....	26

6.16 Profesional Gestión Documental.	27
7. PLANIFICACION Y CONTROL DE OPERACIONES SGSI.....	27
7.1 Administración del riesgo.	27
7.2 Declaración de aplicabilidad.	28
7.3 Indicadores y medición de la seguridad de la información.	28
8. SOPORTE.....	29
8.1 Recursos.....	29
8.2 Toma de conciencia y comunicación.	30
8.3 Información documentada.....	31
8.4 Control operacional.	31
8.5 Gestión de activos.....	32
9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN.....	32
9.1 Auditorías.....	33
9.2 Revisión por la Dirección.....	34
10. MEJORA CONTINUA.....	35
10.1 Hallazgos, no conformidades y acciones correctivas.....	35
11. PROTOCOLO IPV6.....	36
12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	37
13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.....	37
13.1 Continuidad de la seguridad de la información.....	37
13.1.1Rebundancias.....	38
14. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	38
15. VIGENCIA.....	39
16. BIBLIOGRAFIA.....	39

INTRODUCCIÓN

La LOTERÍA DE BOGOTÁ, en cumplimiento a la Norma Técnica Distrital del Sistema Integrado de Gestión para las entidades distritales NTD - SIG 001:2011 y la Norma NTC-ISO-IEC 27001:2013, actualmente reemplazada por la tercera edición NTC-ISO-CEI 27001:2022, inició la implementación del SGSI, como un componente del Sistema Integrado de Gestión de la entidad. Complementariamente, la entidad siguiendo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) sobre la estrategia de Gobierno en línea, adoptó el conjunto de orientaciones y guías técnicas, que proveen y promueven la puesta en marcha, supervisión, mejora y control para la implementación del Modelo de Seguridad y Privacidad de la información (MSPI).

Basados en lo anterior, se crea el presente Manual del SGSI de la LOTERÍA DE BOGOTÁ, como herramienta documental que contiene la planificación e implementación de las políticas, procedimientos, gestión de riesgos, y los controles necesarios para cumplir los requisitos de seguridad y privacidad de la información, a fin de asegurar la confidencialidad, integridad, disponibilidad de los activos de información, y restringir la divulgación no autorizada; agregando valor a la prestación de los trámites y servicios; generando confianza tanto a los servidores públicos, clientes y demás partes interesadas de la LOTERÍA DE BOGOTÁ, a través de la mejora continua.

1. ALCANCE

El manual del SGSI de la LOTERÍA DE BOGOTÁ, cubre de manera transversal a todos los procesos y procedimientos asociados con el Sistema Integrado de Gestión, siguiendo el estándar

de la norma NTC-ISO-CEI 27001:2022, y los elementos complementarios del Modelo de Seguridad y Privacidad de la Información orientados por MINTIC.

2. DEFINICIONES

Para el propósito de este manual se aplican los términos dados en los documentos asociados al modelo de seguridad y privacidad de la información de Mintic, la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP y la Norma NTC-ISO-CEI 27001:2022, además de la política de Gobierno en Digital:

Activo: Cualquier elemento que tenga valor para la organización.

Activo de información: En el contexto de seguridad, digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema específico o a la entidad. (NTC-ISO-IEC 27000).

Caracterización de Proceso: Se refiere a la identificación, personalización y descripción de las características más importantes de un proceso tales como: entradas, actividades, salidas, clientes, etc.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Confidencialidad: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

Disponibilidad: Los activos de información solo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Estrategia: Se centra en definir políticas, objetivos y lineamientos para el logro de la calidad y satisfacción del cliente. Estas políticas y objetivos deben estar alineados a los resultados que la organización desee obtener.

Integridad: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Modelo de Seguridad y Privacidad de Información - MSPI: El Modelo de Seguridad y Privacidad de la Información entrega una guía para construir un SGSI, buscando generar una conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los activos de información de la entidad.

Proceso: Secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr un resultado específico.

Recurso: Son todos aquellos elementos que pueden utilizarse como medios a efectos de alcanzar un fin determinado.

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. (NTC-ISO-IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

SGSI: Conjunto de políticas de administración de la información el cual consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Controles: Medida que modifica o mantiene el riesgo.

Ataque: Intento no autorizado exitoso o fallido de destruir, alterar, deshabilitar, obtener acceso a un activo o cualquier intento de exponer, robar o hacer uso no autorizado de un activo.

Autenticación: Propiedad relacionada con la veracidad que una entidad, es en efecto lo que dice ser.

Información confidencial: Información que no está destinada a estar disponible o divulgada a personas no autorizadas, entidades o procesos.

Información de identificación personal: Cualquier información que pueda utilizarse para establecer un vínculo entre la información y la persona física a la que se refiere dicha información, o esté o pueda estar vinculada directa o indirectamente a una persona física.

SIGLAS Y ABREVIATURAS.

MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones.

MSPI: Modelo de Seguridad y Privacidad de la Información

TIC: Tecnologías de la Información y las Comunicaciones.

VPN: Virtual Private Network - Red Privada Virtual.

WIFI: Wireless Fidelity - Fidelidad inalámbrica.

DASCD: Departamento Administrativo Del Servicio Civil Distrital

SIC: Superintendencia De Industria Y Comercio

CIGYD: Comité Institucional de Gestión Y Desempeño

MAE: Marco de Arquitectura Empresarial

SGSI: Sistemas de Gestión de Seguridad de la Información

3. REFERENCIAS NORMATIVA

Los requisitos, delimitaciones legales y contractuales se describen en el siguiente normograma desarrollado para el SGSI y, en el listado maestro de documentos externos de la LOTERÍA DE BOGOTÁ.

- *Ley 527 de 1999. Ley de Comercio Electrónico y Firmas Digitales.*

- *Ley 594 de 2000. Ley General de Archivos.*
- *Directiva 005 de 2005 de la Alcaldía mayor de Bogotá, “Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital”.*
- *Acuerdo 279 de 2007 Consejo de Bogotá. Lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital*
- *Decreto 296 de 2008. Comité de Gobierno en Línea a la Comisión Distrital de Sistemas.*
- *Resolución 305 de 2008: “Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre”.*
- *Circular No. 058 de 2009 de la Procuraduría General de la Nación Cumplimiento Decreto 1151 de 2008.*
- *Ley 1273 de 2009. Ley de Delitos Informáticos.*
- *CONPES 3701 de 2011: Estrategia Nacional de Ciberseguridad y Ciberdefensa, así como el CONPES 3854 de 2016: “Política Nacional de Seguridad Digital.”*
- *Ley 1581 de 2012: Ley de protección de datos personales; reglamentada parcialmente por el Decreto 1081 de 2015: "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."*
- *Decreto 2364 de 2012. Firma electrónica.*
- *Decreto 2609 de 2012. Gestión documental (Compilado en el 1080 de 2015, Capítulo III).*
- *Circular 005 de 2012 emitida por el Archivo General de la Nación. Recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas en el*

marco de la iniciativa “cero papel”.

- *Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional; reglamentada parcialmente por el Decreto 1081 de 2015: "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República."*
- *Decreto 2573 de 2014: Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.*
- *Decreto 1078 de 2015. Decreto Único Sectorial - Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.*
- *Resolución 3564 de 2015 Reglamentaciones asociadas a la Ley de Transparencia y Acceso a la Información Pública. Ministerio de Tecnologías de la Información y las Comunicaciones.*
- *Circular No. 007 de 2015, Secretaría General de la Alcaldía Mayor de Bogotá. Lineamientos generales para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información.*
- *Conpes 3854 de 2016, Ministerio de Tecnologías de la Información y las Comunicaciones. Política Nacional de Seguridad Digital.*
- *Resolución 004 de 2017 Comisión distrital de Sistemas “Por la cual se modifica la Resolución 305 de 2008 de la CDS”*
- *Circular 37 de 2018 Incidentes de ciberseguridad y modelo de seguridad y privacidad de la información MPSI del MINTIC.*
- *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 las Comunicaciones".

- *Ley 1952 de 2019. 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"; Art. 147.*
- *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.*
- *CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.*
- *Modelo Integrado de Planeación y Gestión – MIPG versión 4, marzo de 2021*
- *Resolución 0500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.*
- *Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones – versión 4. 2021.*
- *Norma ISO/CEI 27001:2022(E) “Seguridad de la información, ciberseguridad y protección de privacidad – Sistemas de gestión de la seguridad de la información”.*
- *Acuerdo 002 de 22 de diciembre de 2023, por el cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.*

4. CONTEXTO DE LA ENTIDAD

En los últimos años el mundo ha atravesado por grandes retos a nivel tecnológico, para no ir muy lejos la pandemia, en este caso, hoy más que nunca la tecnología ha sido el mejor aliado, evidenciando no solo la utilidad sino la eficacia para desarrollar diferentes propósitos a nivel

laboral. En cuanto a la LOTERÍA DE BOGOTÁ, ha sido el pilar y apoyo para el cumplimiento de los objetivos y todos los proyectos trazados por las diferentes áreas, sin embargo, junto a la facilidad del acceso a la información han crecido las amenazas a los sistemas de información, focalizando la necesidad de mitigar las vulnerabilidades a las que nos encontramos expuestos en todo momento.

Por lo anterior, la LOTERÍA DE BOGOTÁ ha dado prioridad al tema de seguridad de la información y en conocimiento de las ventajas que nos aporta las normas internacionales, se encuentra adelantando la implementación y ejecución de las normas NTC ISO 27001:2022 Y NTC ISO 31000:2018, que dan las orientaciones para velar por la integridad disponibilidad, confidencialidad y accesibilidad de la información, al igual que por la gestión de los riesgos de estos pilares.

Dando alcance a los objetivos tanto de la entidad como de las normas mencionadas y con el fin de lograr su efectividad dando cumplimiento, la entidad se encuentra en el desarrollo de actividades para la identificación y actualización de los activos de información, que permitan el adecuado uso de los datos de acuerdo con su clasificación y acceso oportuno según la asignación de roles, disminuyendo el riesgo por el manejo inadecuado de la información.

Los avances alcanzados a nivel del SGSI han permitido de manera visible la protección con respecto a la operación de la entidad al igual que de los datos que se encuentran bajo su responsabilidad, como es la información propia y de terceros, además de desarrollos tecnológicos y sin ser menos importantes, la interconexión que ha permitido que las diferentes plataformas a nivel interno y externo garanticen el desarrollo de la operación de la entidad.

En concordancia con lo expuesto en este contexto, el establecimiento y apropiación por cada uno de los usuarios de la Entidad con respecto a las políticas de la seguridad de la información, permite que se hable un mismo idioma a nivel de Entidad, pues no es un tema aislado la responsabilidad y la importancia que traen consigo la seguridad de la información, considerando

la coyuntura mundial actual, convirtiendo en compromiso y responsabilidad de todos los colaboradores de la entidad, la protección de los datos y no solo de los responsables del SGSI. En la LOTERÍA DE BOGOTÁ se emplea la matriz DOFA – Debilidades, Oportunidades, Fortalezas y Amenazas – para analizar cada uno de los procesos de la entidad. Estas matrices se encuentran documentadas como Contexto Estratégico en el módulo Riesgos con base en las indicaciones del DAFP, así como en el módulo MECI - Administración del Riesgo. Sus resultados permiten identificar los posibles problemas externos e internos que puedan generar riesgos que afecten el cumplimiento de la misión y objetivos institucionales.

Así mismo, dentro de las matrices DOFA de contexto de cada uno de los procesos, se identifican los elementos DOFA generales y que están relacionados con la gestión del riesgo de Seguridad de la Información, los cuales se alinean a la misión y estrategias de la LOTERÍA DE BOGOTÁ, determinando los requisitos de los clientes y las partes interesadas pertinentes a la seguridad de la información, bajo los lineamientos de la norma NTC-ISO-CEI 27001:2022 y MINTIC. Dentro de la Matriz DOFA se identifican estos elementos relacionados, señalándolos con las siglas del Sistema de Gestión de Seguridad de la Información (SGSI).

4.1 Comprensión de las necesidades y expectativas de los clientes y las partes interesadas.

Se identifican los clientes y las partes interesadas que son pertinentes y relevantes del SGSI, los cuales se encuentran identificados en todos los procesos de la entidad, teniendo en cuenta que la Seguridad de la Información es transversal para la entidad y su control y se realiza por medio del Comité Institucional de Gestión y Desempeño (CIGYD). Así mismo, se tienen en cuenta los clientes de la Lotería de Bogotá, como también las agremiaciones o asociaciones en las que participa, y sus proveedores.

5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La LOTERÍA DE BOGOTÁ establece, implementa, mantiene y mejora continuamente el SGSI, por medio de lo establecido en la política, objetivos y en las metas e indicadores de gestión asociados a los objetivos definidos en la política específica del SGSI.

5.1 Documentación del SGSI.

Para abordar la implantación del SGSI se debe desarrollar la siguiente documentación básica: Los procedimientos obligatorios por la NTC-ISO-CEI 27001:2022 (incluyendo los controles del Anexo A de esta norma) y las guías MINTIC, que se documentarán e implementarán de acuerdo con los lineamientos recibidos por la Alta Consejería de las TIC, el Ministerio de las TIC y al cronograma designado por dicha entidad.

- *Activos de información y guías o metodologías para su aplicación.*
- *Definición del alcance.*
- *Definición de una Política de Seguridad.*
- *Identificación, evaluación y tratamiento de riesgos de seguridad de la información, con base en los activos de información.*
- *Elaboración de la Declaración de Aplicabilidad de controles y requisitos o herramienta de autodiagnóstico de MINTIC:*
- *Desarrollo de programas de socialización y sensibilización en términos de seguridad de la información.*
- *Elaboración de procedimientos y documentación asociada.*

5.2 Política general del SGSI.

La LOTERÍA DE BOGOTÁ establece la política general de la seguridad de la información del SGSI, y sus políticas complementarias, las cuales son adecuadas al propósito de la organización y busca garantizar la identificación y protección de los activos de información, implementando los mecanismos y controles para asegurar su confidencialidad, integridad, disponibilidad, y evitar la divulgación no autorizada de la información institucional acorde con sus riesgos.

Las Políticas aplican en todo el ámbito de la LOTERÍA DE BOGOTÁ, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros, encontrándose alineada con el enfoque de la gestión del riesgo, señalado en el documento CONPES 3854 de 2016, y su reconocimiento como uno de los elementos más importantes para abordar la seguridad digital, involucrando a las partes interesadas y asegurando una responsabilidad compartida.

Así mismo, las Políticas cubren todos los aspectos administrativos y de control que deben ser cumplidos por los funcionarios y contratistas de la LOTERÍA DE BOGOTÁ para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: Consciente de las necesidades derivadas de sus actividades, la LOTERÍA DE BOGOTÁ adopta el Sistema de Gestión de la Seguridad de la Información como una herramienta para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, administrando los riesgos, cumpliendo con la legislación vigente y generando una cultura de seguridad de la información en los servidores, colaboradores públicos y demás partes interesadas.

5.3 Objetivo general

Mantener la confidencialidad, integridad, disponibilidad de los activos de información, y la protección de datos personales, mediante la gestión de los riesgos, que permita establecer un marco de confianza a las partes interesadas en concordancia con la misión y visión de la entidad.

5.4 Objetivos específicos

1. *Salvaguardar los activos de información, con base en los criterios de confidencialidad, integridad y disponibilidad, mediante la implementación de controles en los procesos de la entidad de manera coordinada con las partes interesadas.*
2. *Proteger el talento humano, la información y los recursos tecnológicos utilizados por la LOTERÍA DE BOGOTÁ frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.*
3. *Formular lineamientos en seguridad de la información para la LOTERÍA DE BOGOTÁ que permitan proteger los activos de información, y la materialización de riesgos, de tal manera que se preserve su confidencialidad, integridad y disponibilidad, de acuerdo con el nivel de criticidad establecido en la clasificación y valoración de dichos activos realizada en la entidad y teniendo en cuenta los controles establecidos sobre los riesgos.*
4. *Definir directrices para el correcto uso de los componentes de hardware, software, información física e información digital de la LOTERÍA DE BOGOTÁ, con el fin de contribuir a la mitigación del riesgo de ocurrencia de incidentes de seguridad de la información.*

5. *Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de sus derechos.*
6. *Establecer medidas de protección para las comunicaciones y manejo de información, que involucre datos personales, tanto internas como externas, para garantizar la confidencialidad y protección de esta información.*
7. *Sensibilizar y entrenar al personal de la entidad en el SGSI.*

5.5 Políticas específicas y complementarias de seguridad y privacidad de la información.

Se cuenta con un compendio general de Políticas de Seguridad de la información complementarias, las cuales dan los lineamientos que se deben cumplir en la LOTERÍA DE BOGOTÁ, estas políticas se encuentran documentadas y se pueden consultar tanto en la página web de la entidad como en la herramienta que actúa como repositorio interno.

5.6 Compromiso y liderazgo de la Dirección.

La Alta Dirección de la LOTERÍA DE BOGOTÁ está comprometida con la influencia y responsabilidad directa del SGSI.

Se cuenta con el compromiso y concurso de todos los servidores públicos de la entidad, para el mantenimiento y mejora continua en nuestro SIG, los procesos y productos, para así cumplir con las necesidades y expectativas de nuestros clientes y partes interesadas, tal y como está documentado en el Manual del SIG.

De igual manera, a través de la implementación y seguimiento del Plan Estratégico Institucional 2021-2024, será imprescindible la participación y esfuerzo de todo el capital humano de la entidad, alineándose con la estrategia definida y actuando con el compromiso no solo de hacer

las cosas bien, sino de hacerlas con una permanente preocupación de satisfacer las necesidades de sus usuarios y con la seguridad y la confianza del beneficio del Distrito Capital.

La Alta Dirección de la LOTERÍA DE BOGOTÁ por medio de la oficina de control interno garantizará por medio de las auditorías que los objetivos establecidos y medidos con sus respectivas metas e indicadores corresponden con la Política General implementada y esté alineada al SGSI.

La LOTERÍA DE BOGOTÁ establece como máxima autoridad del SGSI al Comité del Sistema Integrado de Gestión quien es responsable de la orientación estratégica para la administración de los activos de Información, la sostenibilidad y mejora del Sistema en la Entidad. En este sentido, el liderazgo está en cabeza de la Alta Dirección de la LOTERÍA DE BOGOTÁ en cumplimiento de las funciones establecidas en el Artículo 2 de la Resolución LOTERÍA DE BOGOTÁ No. 00291 de 2017 *"Por la cual se modifica parcialmente la Resolución 176 de 2015 "Por la cual se crea el Comité del Sistema Integrado de Gestión, y se dictan otras disposiciones"* y la resolución 362 de 2016 *"Por la cual se modifica parcialmente la Resolución 176 de 2015"*; y como líder del SGSI a la Dirección de Planeación y Sistemas de Información Ambiental.

El numeral 4.3 de la Norma Técnica Distrital del SIG establece los requisitos en materia de Compromiso de la Alta Dirección, y en su literal c dispone que *"La alta dirección debe designar uno o varios miembros del grupo directivo con responsabilidades específicas en el Sistema Integrado de Gestión y con independencia de otras responsabilidades que le sean asignadas"*, en este sentido la LOTERÍA DE BOGOTÁ documentó en la Resolución LOTERÍA DE BOGOTÁ No. 176 de 2015 Artículo 9, que cuando se trate de un tema específico asociado a un sistema en particular, el representante de cada sistema ejercerá la relatoría necesaria para la sesión correspondiente, como apoyo a la Secretaria Técnica, es así como para el SGSI, será la Dirección de Planeación y Sistemas de Información Ambiental - DPSIA, quien desarrolle estas tareas.

La Alta Dirección asegura que las responsabilidades y autoridades para los roles pertinentes a la seguridad y privacidad de la información se asignen y comuniquen correctamente.

6. ROLES Y RESPONSABLES

Las actividades por realizar en cuanto a la Seguridad de la Información por parte de los funcionarios y colaboradores de la Lotería de Bogotá, deben ser asignadas a las personas con el conocimiento y las competencias pertinentes.

Lo anterior permitirá, que el establecimiento de roles emita las responsabilidades que acarrearán cada uno de los miembros del equipo del MSPI, minimizando la posibilidad de situaciones fuera de la responsabilidad de la que cada uno se empodera.

Hay que asegurar que la actividad instaurada dentro de la etapa de planeación del MSPI, tenga un responsable para quien la ejecución sea clara, ya que es el fin mismo del entendimiento de los roles y responsabilidades de cada miembro del equipo en cuanto a la Lotería de Bogotá.

6.1 Identificación de los responsables

Considerando la importancia del desarrollo del MSPI y en pro de garantizar el apoyo desde el inicio de la planeación, se hace necesario la participación de los funcionarios y colaboradores de alto nivel, que se encontrarán vinculados, con el fin de lograr la implementación del modelo de gestión de seguridad de la información de forma satisfactoria para la Lotería de Bogotá.

Los representantes de alto nivel de la Lotería de Bogotá mediante la política deben, identificar y establecer la organización de un equipo de trabajo que se haga responsable de la implementación del Modelo de Seguridad de la Información, definiendo el perfil y el rol, los cuales deben ser dados a conocer a los responsables, y su aprobación se debe dar en el marco del Comité de Gestión y Desempeño.

6.2 Equipo de gestión al interior de la Lotería de Bogotá

El Oficial de Seguridad o quien haga sus veces, liderará las actividades necesarias para planear, implementar y hacer seguimiento a las acciones necesarias, para adoptar el Modelo de Seguridad y Privacidad de la Información al interior de la Lotería de Bogotá; así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este, con el respaldo de la alta dirección.



Elaboración propia

6.3 Responsable de la Seguridad de la Información o quien haga sus veces para la Lotería de Bogotá

- *Fomentar la implementación de la Política de Gobierno Digital*
- *Asesorar a la entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la Lotería de Bogotá de conformidad con la regulación vigente.*

- *Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la Lotería de Bogotá.*
- *Realizar la estimación, planificación y cronograma de la implementación del MSPI.*
- *Liderar la implementación y hacer seguimiento a las tareas y cronograma definido.*
- *Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.*
- *De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información.*
- *Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.*
- *Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.*
- *Definir e implementar en coordinación con las dependencias de la Lotería de Bogotá, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.*
- *Apoyar a los procesos de la Lotería de Bogotá, en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información.*
- *Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la Lotería de Bogotá.*

- *Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.*
- *Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.*

6.4 Comité de Gestión y Desempeño de la Lotería de Bogotá

- *Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:*
- *Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad y privacidad de la información.*
- *Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.*
- *Aprobar acciones y mejores prácticas que en la implementación del MSPI.*
- *Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.*
- *Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.*

6.5 Oficina asesora Jurídica de la Lotería de Bogotá

- *Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.*
- *Brindar asesoría al Comité de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.*
- *Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.*
- *Representar a la entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.*
- *Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.*

6.6 Gestión del Talento Humano de la Lotería de Bogotá

- *Controlar y salvaguardar la información de datos personales del personal de planta de la Lotería de Bogotá, en concordancia con la normatividad vigente.*
- *Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.*

- *Fomentar la cultura de seguridad de la información.*

6.7 Oficina de Control Interno

- *Definirá dentro de su plan anual de auditoría, las auditorías necesarias respecto al MPSI.*
- *Evaluará de forma independiente, el avance y los controles implementados del MPSI.*
- *Como tercera línea de defensa, hará seguimiento y evaluará los riesgos de Seguridad Digital y la eficacia de sus controles.*
- *En los casos en los que se requiera y según lo establecido en el MPSI, apoyará y asesorará la evaluación del MPSI.*

6.8 Separación de deberes

Todo aquel que tenga acceso a la información de la LOTERÍA DE BOGOTÁ, debe tener claramente definidas sus funciones u obligaciones, con el fin de reducir el uso no autorizado, indebido o accidental de los activos de información.

Todos los sistemas de información de la entidad deben implementar reglas de acceso a los mismos, de tal forma que existan roles entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

6.9 Contacto con autoridades y grupos de interés

La LOTERÍA DE BOGOTÁ mantendrá contacto con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes.

Adicionalmente, la Oficina de Gestión Tecnológica e Innovación cuenta con un directorio actualizado de autoridades y grupos de interés.

La Oficina de Gestión Tecnológica e Innovación mantendrá contacto con grupos especializados, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior, con el fin de estar al día con la información relacionada con la seguridad de la información, mejores prácticas y recibir advertencias de actualizaciones, ataques y vulnerabilidades del software y firmware utilizado en la LOTERÍA DE BOGOTÁ.

6.10 Equipo técnico del SGSI

El equipo Técnico del SGSI, se activa en los casos en que sea necesario, ya sea por materialización de amenazas o de riesgos, o situaciones y necesidades relacionadas con Seguridad de la Información. Los integrantes del equipo serán convocados según la necesidad presentada por el Oficial de Seguridad de la Información (o quien haga sus veces) y su aprobación será dada por el/la jefe Oficina de Gestión Tecnológica e Innovación:

- *Jefe Oficina de Gestión Tecnológica e Innovación*
- *CISO: Oficial de seguridad de la información o quien haga sus veces*
- *Profesional Sistemas de Información*
- *Profesional Infraestructura TI*
- *Profesional Gestión Documental.*
- *Profesional Servicios Tecnológicos*
- *Servidores/colaboradores públicos y partes interesadas*

Estos roles pueden variar dentro de la LOTERÍA DE BOGOTÁ, según la disponibilidad del personal que ejecuta cada actividad relacionada con el rol; para los casos en que no exista dicho rol, se deberá buscar el homologado o quien tenga la actividad relacionada con el tema a tratar. A

continuación, se describen los roles dentro del Equipo técnico, cabe mencionar que estos roles complementan y apoyan la gestión sobre el SGSI y pueden activarse en caso de que ser necesario. Así mismo, en caso de ser requerido se podrá convocar a funcionarios y colaboradores de otros procesos, para contar con su apoyo y conocimiento.

6.11 Jefe Oficina de Gestión Tecnológica e Innovación:

- *Aprobar las propuestas realizadas para la planeación, implementación, operación, monitoreo, mantenimiento, revisión y mejora continua del SGSI.*
- *Aprobar las propuestas del SGSI, respecto a la gestión de riesgos de seguridad de la información requeridas para la Entidad.*
- *Gestionar los recursos, para crear, implementar y promover las estrategias y políticas establecidas en el SGSI.*

6.12 Oficial de seguridad de la información o quien haga sus veces

- *Aplicar conocimientos, habilidades, herramientas y técnicas a las actividades propias del proyecto de implementación de Seguridad de la información, de manera que cumpla las necesidades y expectativas de los interesados en el proyecto.*
- *Identificar la brecha entre el Modelo de seguridad y privacidad de la información MSPI y la situación actual de la entidad en los aspectos relacionados a seguridad de la información.*
- *Generar el cronograma de la implementación del SGSI alineado al Modelo de Seguridad y privacidad de la información.*
- *Coordinar las actividades del equipo implementador de la seguridad de la información.*

- *Encaminar el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad, lo anterior por medio del instrumento de autodiagnóstico de Mintic.*
- *Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos que se puedan presentar en la implementación para darle solución oportuna y escalar al Comité de gestión y desempeño en caso de ser necesario.*
- *Velar por el mantenimiento de la documentación del SGSI.*
- *Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre la implementación del SGSI.*

6.13 Profesional infraestructura TI.

- *Realizar la configuración de los diferentes equipos activos de comunicaciones de la plataforma de redes de la LOTERÍA DE BOGOTÁ, con base en las políticas de seguridad de la información, para minimizar riesgos que afecten el funcionamiento normal de la Entidad.*
- *Documentar y actualizar periódicamente los esquemas de red de los diferentes dispositivos de comunicación, las implementaciones actuales y futuras de los equipos con que cuenta la LOTERÍA DE BOGOTÁ; para garantizar que se encuentren actualizados, con el fin de gestionar los riesgos de seguridad de información asociados al acceso, trazabilidad, modificación o pérdida de información, en los que su materialización atente contra la disponibilidad, integridad y confidencialidad de la información.*
- *Monitorear la infraestructura de la Entidad a fin de realizar los cambios eventuales requeridos para mantener la disponibilidad de los diferentes servicios de TI que presta la entidad y garantizar la continuidad del negocio y su seguridad de información.*

- *Realizar y documentar las recomendaciones técnicas para fortalecer la infraestructura tecnológica de la LOTERÍA DE BOGOTÁ, a nivel de seguridad de información.*

6.14 Profesional servicios tecnológicos o quien haga sus veces. (Web Master, profesional de apoyo de la Oficina)

- *Monitorear la disponibilidad de los portales WEB, aplicando buenas prácticas de seguridad y protección de la información,*
- *Realizar las copias de respaldo de los servicios tecnológicos, de la LOTERÍA DE BOGOTÁ de acuerdo con los procedimientos y protocolos establecidos.*
- *Apoyar el tratamiento de los eventos e incidencias de seguridad de la información y gestión su mitigación.*
- *Aplicar las políticas de seguridad y privacidad de la información y los indicado en la Política de Gobierno Digital.*
- *Participar junto con el grupo de infraestructura de TI de la Entidad, pruebas de vulnerabilidad sobre los activos de Seguridad de Información.*

6.15 Profesional responsable de los sistemas de información (Web Master, profesional de apoyo de la Oficina)

- *Monitorear el uso de los sistemas de información de la entidad y el portal web, para detectar vulnerabilidades que afecten la gestión de la información.*
- *Realizar seguimiento a la trazabilidad generada por un sistema de información y portal web para controlar su correcto flujo e identificación de posibles alteraciones.*

6.16 Profesional Gestión Documental.

- *Asegurar que los instrumentos archivísticos publicados en la página web cumplan con las normas y protocolos establecidos en la gestión documental.*
- *Alinear las políticas archivísticas con las políticas del SGSI de la LOTERÍA DE BOGOTÁ*
- *Integración y alineación de las tablas de retención con el SGSI.*
- *Participar en la identificación clasificación y valoración de los inventarios de activos de información y su respectiva influencia en la gestión documental con relación a la seguridad de la información.*

7. PLANIFICACION Y CONTROL DE OPERACIONES SGSI

Las etapas definidas para el desarrollo y la implementación del SGSI son:

1. *Planear y documentar el sistema.*
2. *Implementar el sistema.*
3. *Evaluar el sistema a través de auditorías internas y externas. Y Adelantar actividades de autoevaluación como las reuniones de seguimiento o la aplicación de instrumentos de autoevaluación.*
4. *Mejorar continuamente la eficacia del sistema a través del análisis de datos*

7.1 Administración del riesgo.

La administración del riesgo (lo cual incluye la identificación, clasificación, valoración y tratamiento de los riesgos en Seguridad de la Información), se realizará de acuerdo con el procedimiento Administración de Riesgos y Oportunidades: 126PG01-PR09. Además, se articula con la metodología de Activos de Información aplicada en la entidad, cumpliendo con lo indicado

por el DAFP. Y partiendo del análisis sobre las amenazas y vulnerabilidades asociadas a los activos de Información.

7.2 Declaración de aplicabilidad.

La Declaración de Aplicabilidad es una herramienta que lista los objetivos y controles que se van a implementar en la Entidad. Para el caso del SGSI de la LOTERÍA DE BOGOTÁ se enlistan los controles de seguridad establecidos en el Anexo A de la norma estándar NTC-ISO-IEC 27001:2013, actualmente reemplazada por la tercera edición NTC-ISO-CEI 27001:2022. Y se utiliza el instrumento de diagnóstico del MSPI suministrado por MINTIC.

La información que convierte este registro en un documento vivo es la determinación del estado de cada uno de los controles y la evidencia de dicho estado. Por lo anterior, esta Declaración de Aplicabilidad debe ser alimentada periódicamente con las evidencias y evoluciones del SGSI, o contar con el instrumento de diagnóstico del MSPI suministrado por MINTIC actualizado, el cual también lista los controles a aplicar, y califica el nivel de cumplimiento de cada uno de ellos.

7.3 Indicadores y medición de la seguridad de la información.

Con el fin de verificar el cumplimiento de la implementación de los objetivos específicos y el compromiso adquirido por la entidad en la política general del SGSI se establecen los indicadores, de acuerdo con la siguiente tabla:

Objetivo	Indicador	Tipología	Meta por vigencia
Propender por la atención y asistencia oportuna a las necesidades de los colaboradores de la LOTERÍA DE BOGOTÁ en temas de TI.	((No. De incidentes atendidos) / (No. De incidentes registrados en la mesa de ayuda)) *100	Eficiencia	Atención del 100% de los incidentes recibidos.
Sensibilizar a los colaboradores de la LOTERÍA DE BOGOTÁ sobre el uso responsable de la información y el manejo de las TI.	((No. De actividades de sensibilización sobre TI realizadas) / (No. De actividades de sensibilización sobre TI programadas)) *100	Efectividad	Realización del 100% de las actividades de sensibilización programadas.
Proteger y administrar los activos de información, como base fundamental del SGSI, de conformidad con lo señalado en la normatividad vigente y las disposiciones de cada área.	((No. de actualizaciones realizadas en el registro de activos de información) / (No. de procesos al interior de la LOTERÍA DE BOGOTÁ)) *100	Efectividad	Consolidar un registro de activos de Información actualizado y cumpliendo con las necesidades relacionadas con salvaguardar de manera adecuada la información de la entidad. todos los procesos de la LOTERÍA DE BOGOTÁ.

8. SOPORTE

8.1 Recursos.

La LOTERÍA DE BOGOTÁ proporciona los recursos necesarios para el establecimiento, implementación, mantenimiento y mejoramiento continuo del SGSI.

La Alta Dirección garantizará los recursos necesarios. Para ello, por medio de la Oficina de Gestión Tecnológica e Innovación, mantendrá y fortalecerá los sistemas de información y tecnología adecuados, administrará y conservará los documentos de archivo producidos en el

ejercicio de su gestión, mantendrá recursos humanos idóneos y competentes, identificará y controlará continuamente sus aspectos significativos, respondiendo con la satisfacción de sus clientes y partes interesadas promoviendo un ambiente de responsabilidad social y cultura de seguridad de la Información.

8.2 Toma de conciencia y comunicación.

La LOTERÍA DE BOGOTÁ desarrolla los procedimientos necesarios para la comunicación organizacional interna y externa, lo anterior con el fin de promover la construcción de una visión compartida, facilitar los procesos de rendición de cuentas y suministrar información de manera oportuna.

Los servidores y colaboradores tendrán acceso a los medios y recursos para adelantar las sensibilizaciones relacionadas con Seguridad de la Información, logrando toma de conciencia y actualización sobre las políticas y procedimientos pertinentes a su labor en la LOTERÍA DE BOGOTÁ. Esto se logrará a través de las actividades planteadas en cada vigencia en el Plan Institucional de Capacitación, para fortalecer la cultura de Seguridad de la Información.

El contenido de la comunicación del SGSI parte de desarrollar diferentes actividades, como campañas, talleres y charlas de socialización referentes al SGSI, que ayuden a la sensibilización y capacitación sobre seguridad de la información, además deberá:

- *Definir los temas para las sensibilizaciones en seguridad de la información, de acuerdo con el público objetivo.*
- *Establecer la metodología que les permita evidenciar cuáles son las necesidades temáticas de Seguridad de la Información para la LOTERÍA DE BOGOTÁ.*
- *Construir materiales para sensibilización y entrenamiento.*

- *Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades de la LOTERÍA DE BOGOTÁ.*

El proceso de difusión irá de acuerdo con la implementación de lo definido en la planeación del SGSI. Se utilizarán los canales de comunicación y las diferentes herramientas de difusión que posee la LOTERÍA DE BOGOTÁ fomentando la cultura de la seguridad y privacidad de la información de manera didáctica y amena, favoreciendo el cumplimiento de las políticas establecidas dentro del SGSI. La comunicación será a todos los funcionarios, contratistas y terceros de la LOTERÍA DE BOGOTÁ.

8.3 Información documentada.

La LOTERÍA DE BOGOTÁ, genera la documentación necesaria y asociada al SGSI, como lo es:

- *Manual Del Sistema De Gestión De La Seguridad De La Información / Políticas de Seguridad de la Información.*
- *Guías y herramientas relacionados con el SGSI.*
- *Procedimientos y documentos reglamentarios.*

8.4 Control operacional.

Se establecerán acuerdos de nivel de servicio que permitan mitigar posibles riesgos de seguridad de la información en la entidad. Estos se aplicarán en los contratos que apoyen la operación en términos de Seguridad de la Información, como por ejemplo firewall, antivirus y plataformas de correos electrónicos.

8.5 Gestión de activos.

Es necesario tener claro que un activo es cualquier elemento que tenga un valor para la LOTERÍA DE BOGOTÁ, y en términos de seguridad digital estos activos son elementos tales como aplicaciones, servicios Web, redes, información física o digital, Tecnologías de la Información o Tecnologías de la Operación. Para identificarlos, se documentan por medio de un inventario de activos, con el fin de protegerlos adecuadamente, y garantizar su funcionamiento. Esta identificación y valoración de activos, se debe adelantar por la Primera Línea de Defensa, es decir por los líderes de Proceso y su equipo de trabajo, esto con el apoyo y asesoramiento del equipo de Seguridad de la Información de la LOTERÍA DE BOGOTÁ, articulando estas actividades con los riesgos de seguridad de la Información. Para adelantar esta actividad, se debe tener en cuenta la guía de identificación de activos de información de la Lotería de Bogotá. Esta gestión sobre los activos en la LOTERÍA DE BOGOTÁ se basa en el estándar NTC-SO-IEC 27001:2022 y la guía No. 5 de Gestión y Clasificación de activos de MINTIC. Para este fin, la LOTERÍA DE BOGOTÁ cuenta con su metodología de Activos de información y los instrumentos para identificar diligenciar y calificar estos activos.

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Además de la medición y seguimiento con los Indicadores, se podrá evaluar el desempeño de la seguridad de la información y la eficacia del SGSI, a partir de las herramientas de verificación establecidas en el ciclo PHVA de cada una de las caracterizaciones de los procesos de la entidad como: Auditorias, Autoevaluación de la Gestión, Encuestas, Revisión por la Dirección, Derechos de petición, quejas y reclamos.

Adicional a las herramientas internas de verificación, se desarrollarán las metodologías de análisis y evaluación que dispongan los entes de control y agentes externos, como la Consejería distrital de las TIC y el Ministerio de las TIC, con el fin de establecer el nivel de madurez que tenga la entidad frente a la seguridad y privacidad de la información. Para tal fin, se utiliza la herramienta de autoevaluación para la identificación del nivel de madurez de la entidad para el Modelo de Seguridad y Privacidad de la información de MINTIC, la cual se debe actualizar mínimo de forma semestral.

9.1 Auditorías.

La LOTERÍA DE BOGOTÁ a través de su proceso de evaluación independiente a la gestión, fomenta el autocontrol e identifica oportunidades de mejoramiento continuo a partir de las evaluaciones adelantadas por medio de auditorías internas y seguimientos. Corresponde a la Oficina de Control Interno de la LOTERÍA DE BOGOTÁ, la realización de las Auditorías Internas, las cuales se planifican, ejecuta e informan los resultados de dichas evaluaciones, a fin de mantener y mejorar el SGSI.

El equipo Auditor deberá conocer de manera integral el MSPI de Mintic, la norma NTC-ISO-IEC 27001:2022, y las políticas de seguridad de la información de la LOTERÍA DE BOGOTÁ y contar con certificados como Auditores Internos por un ente certificador autorizado. En los casos que la OCI requiera el apoyo de un experto técnico para la realización de la auditoría, se podrá solicitar acompañamiento del personal que requiera, siempre garantizando la confidencialidad, integridad y disponibilidad de la información de la LOTERÍA DE BOGOTÁ.

CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

- *Controles sobre auditorías de sistemas de información*

- *Para la ejecución de auditorías a los sistemas de información se deben tener en cuenta las siguientes consideraciones:*
- *Los requisitos de auditoría para acceso a sistemas y a datos se deben acordar con el jefe de área y/o dependencia involucrada.*
- *El alcance de las pruebas técnicas de auditoría se debe acordar y controlar.*
- *Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales.*
- *Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.*

9.2 Revisión por la Dirección.

Se realizará la revisión por la Dirección con el objeto de asegurar la conveniencia, adecuación, eficacia, eficiencia y efectividad del SGSI como integrante del Sistema de Integrado de Gestión de la LOTERÍA DE BOGOTÁ, además los resultados se deberán retener y mantener como información documentada.

Los resultados de la revisión por la Dirección deben incluir todas las decisiones y acciones relacionadas con la mejora de la eficacia, eficiencia y efectividad del Sistema Integrado de Gestión y sus procesos, la mejora del producto o servicio en relación con los requisitos del cliente, las necesidades de recursos, posibles cambios en la política, objetivos, metas y otros elementos de la gestión, coherentes con el compromiso de mejora continua.

10. MEJORA CONTINUA

La LOTERÍA DE BOGOTÁ busca implementar de manera adecuada y efectiva el SGSI, por medio de la utilización, cumplimiento y socialización de la Política General, las interiorización y aplicación de las políticas específicas de Seguridad de la Información, de manera articulada e integrada con el Sistema de Gestión de Calidad de la LOTERÍA DE BOGOTÁ.

Producto del seguimiento, evaluación, análisis y monitoreo de los indicadores y metas, se evaluarán y analizarán estos resultados, para corregir de ser necesario, los errores cometidos, así como mejorar las acciones llevadas a cabo en las fases anteriores, dando cumplimiento al plan de mejoramiento derivado de las auditorías realizadas sobre seguridad y privacidad de la información.

La mejora continua es uno de los elementos más importantes de un sistema de gestión y con ella la implementación de acciones correctivas y preventivas que eliminen las causas de las situaciones reales o potenciales, que afecten la eficacia del sistema. Con estas acciones u oportunidades de mejora desarrolladas, se ayudará a prevenir posibles no conformidades, además se identificarán las posibles modificaciones a los riesgos encontrados y se buscará su correcto manejo de mitigación.

10.1 Hallazgos, no conformidades y acciones correctivas.

El establecimiento de las acciones correctivas debe buscar la eliminación de las causas que conllevaron a la identificación de un hallazgo, no conformidad u observaciones. Para la mejora continua del SGSI, se deben implementar las acciones necesarias, revisando la eficiencia de las acciones correctivas llevadas a cabo. Así mismo, es necesario generar acciones preventivas

para que la situación no se materialice de nuevo. Para este fin, es necesario definir las acciones en el formato de plan de mejoramiento aprobado por la entidad.

Los responsables de procesos y/o jefes de dependencia evaluarán, en coordinación con la Oficina de Control Interno, la pertinencia de la reformulación de las acciones que se encuentren vencidas, hasta garantizar la eliminación de la causa del hallazgo.

11. PROTOCOLO IPV6

Para facilitar el entendimiento, se puede colocar como ejemplo que una dirección IP es un número telefónico o una dirección de una calle. Cuando hay una conexión a Internet, el dispositivo (computadora, teléfono celular, tableta) tiene asignado una dirección IP, así como también cada sitio que se visita tiene una dirección IP. El sistema de direccionamiento que se ha estado usando desde que nació Internet es denominado IPv4. Por temas de capacidad y normatividad, se encuentra en transición a sistema de direccionamiento IPv6. La razón por la cual se debe adelantar estas actividades de transición es debido a que Internet necesita un rango más amplio de direcciones que las que provee IPv4, teniendo en cuenta que IPv6 proporciona exponencialmente un rango mucho más amplio de IP.

Adicional a los controles y dominios de la NTD ISO 27001:2022, la LOTERÍA DE BOGOTÁ en cumplimiento con los componentes solicitados por el Ministerio de las TIC, realizará un análisis y transición de IPV4 a IPV6; basados en la siguiente situación real: “Desde hace más de tres décadas, las redes de telecomunicaciones han venido creciendo exponencialmente generando mayor demanda de servicios y oportunidades en la red mundial de internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido

que hacerlo con direcciones de internet que permiten establecer conexiones para cada elemento conectado a la red, estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en estos momentos entraron a una fase de agotamiento final”.

Debido a lo expuesto anteriormente, la LOTERÍA DE BOGOTÁ adelanta actividades para lograr la transición e implementación necesaria, con base en los recursos y capacidades disponibles por la entidad. Así mismo, para cumplir con los objetivos de innovación tecnológica que exige el país, es necesario seguir las instrucciones descritas en la Circular 002 del 6 de julio de 2011 del Ministerio de Tecnologías de la Información y las Comunicaciones, que busca promover la adopción de IPv6 en Colombia.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La entidad realizará el seguimiento a los incidentes de seguridad de la información de acuerdo con las directrices del procedimiento Gestión de Incidentes de Seguridad de la Información.

13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

13.1 Continuidad de la seguridad de la información

La entidad planificará e implementará la continuidad del negocio (PCN) teniendo en cuenta el talento humano, recursos tecnológicos, activos de información y los procesos críticos de la entidad, además de la continuidad de la seguridad de la información. Se debe garantizar la disponibilidad de los servicios con un rango no inferior a 95%.

La entidad realizará pruebas periódicas (al menos anualmente) al plan de continuidad del negocio y de continuidad de la seguridad de la información implementados, con el fin de asegurar que serán válidos y eficaces durante situaciones adversas.

13.1.1 Redundancias

La entidad establecerá e implementará un plan de contingencia institucional, como parte del Plan de Continuidad de Negocio con el fin de asegurar la continuidad de las instalaciones de procesamiento de información. Así mismo, debe solicitar a sus diferentes contratistas (proveedores), que con base en la disponibilidad se garantice la continuidad de los servicios ofrecidos. La redundancia se hace por medio de las copias de seguridad y versionamiento de los sistemas de información.

14. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Toda violación de estas políticas se debe notificar a la Oficina de Gestión Tecnológica e Innovación a través de correo electrónico mesadeservicio@loteriadebogota.com

Asimismo, se deben notificar situaciones tales como: personas ajenas a la LOTERÍA DE BOGOTÁ sin identificación y sin acompañamiento en las oficinas, correos maliciosos o sospechosos, uso de software ilegal, divulgación, alteración y robo de información.

15. VIGENCIA

El presente manual tendrá vigencia a partir de la fecha de aprobación, la cual se realizó en sesión del Comité Institucional de Gestión y Desempeño de enero de 2025.

16. BIBLIOGRAFIA

ICONTEC. (2013). *Norma Técnica ntc-iso/iec Colombiana 27001*. Colombia.

ISO/IEC. (2012). *NTC-ISO/IEC 27032, Information technology - Security techniques - Guidelines for cybersecurity*.

ISO/IEC. (2018a). *NTC-ISO/IEC 27000, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión General y Vocabulario. 2018*, 1–38. Retrieved from http://k504.khai.edu/attachments/article/819/ISO_27000_2014.pdf

ISO/IEC. (2018b). *NTC-ISO/IEC 27005, Tecnología de la Información. Tecnicas de Seguridad. Gestión del Riesgo en Seguridad de la Información. (Vol. 2018)*.

ISO/IEC. (2018c). *NTC-ISO/IEC 31000, Gestión del Riesgo. Directrices. 2018*, 1–30.

OWASP PROJECT. (2019). *SQL Injection - OWASP*. Retrieved December 9, 2019, from https://www.owasp.org/index.php/SQL_Injection

MANUAL DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
CODIGO:	MA340-647-1	VERSIÓN: 1
ELABORÓ	REVISÓ	APROBÓ
Luis Alejandro Ruiz	Yolanda Patricia Gallego Galvis	Comité de Gestión y Desempeño
Profesional Especializado OGTI	Profesional Especializado OGTI	

REGISTRO DE MODIFICACIONES		
VERSIÓN	FECHA	DESCRIPCIÓN MODIFICACIÓN
01	19-05-2025	Versión inicial