POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN

LOTERÍA DE BOGOTÁ

OFICINA DE GESTIÓN TECNOLÓGICA E INNOVACIÓN

Abril 21 de 2025

Tabla de contenido

INTRODUCCIÓN 4
1. Política general del SGSI. 5
1.1 Política general del sistema de gestión de seguridad de la información: 5
2. OBJETIVO 5
2.1. Objetivos específicos 6
3. ALCANCE 6
4. NORMATIVIDAD (BASE LEGAL) 7
5. DEFINICIONES 8
6. RESPONSABILIDAD Y AUTORIDAD 11
6.1 Roles de seguridad de la información 12
7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 12
7.1 Seguridad de los recursos humanos 12
7.1.1 Vinculación, desvinculación y cambio de cargo 13
7.1.2 Capacitación y entrenamiento en seguridad de la información 13
7.1.3 Procesos disciplinarios 14
7.1.4 Intercambio de información 14
7.2 Seguridad de la información en la gestión de contratos 14
7.3 Dispositivos Móviles Y Teletrabajo O Trabajo En Casa 15
7.3.1 Dispositivos móviles 15
7.3.2 Teletrabajo o trabajo en casa 15
7.4 GESTIÓN DE ACTIVOS 15
7.4.1 Inventario de activos 16
7.4.2 Asignación de activos 16
7.4.3 Uso aceptable de los activos 17
7.4.4 Devolución de activos 17
7.4.5 Uso de equipos de cómputo 17
7.4.6 Uso de internet 18
7.4.7 Uso del correo institucional 19
7.5 Gestión de medios removibles (unidades de almacenamiento) 21
7.5.1 Almacenamiento En la Nube y carpetas compartidas 22
7.6 Clasificación de la información 23
7.6.1 Disposición de los medios 23

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

7.6.2 Transferencia de medios físicos 24
7.7 CONTROL DE ACCESO 24
7.7.1 Política de control de acceso a los sistemas de información. 24
7.7.2 Acceso a redes y a servicios en red 25
7.7.3 Gestión de acceso de usuarios 26
7.7.4 Uso de Información de autenticación secreta (Responsabilidades de los Usuarios) 26
7.7.5 Control de acceso a sistemas y aplicaciones 27
7.8 CONTROLES CRIPTOGRÁFICOS 27
7.9 SEGURIDAD FÍSICA Y DEL ENTORNO 28
7.9.1 Áreas seguras 28
7.9.2 Ubicación y protección de los equipos 29
7.9.3 Servicios de suministro 29
7.9.4 Seguridad del cableado 29
7.9.5 Mantenimiento de equipos 29
7.9.6 Seguridad de equipos y activos fuera de las instalaciones 30
7.9.7 Disposición segura o reutilización de equipos 30
7.9.8 Política de equipo desatendido, escritorio y pantalla limpios 31
7.10 SEGURIDAD DE LAS OPERACIONES 31
7.10.1 Documentación de procedimientos operativos 31
7.10.2 Control de cambios 31
7.10.3 Gestión de capacidad 32
7.10.4 Separación de los ambientes 32
7.11 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS 32
7.12 COPIAS DE RESPALDO 33
7.13 REGISTRO Y SUPERVISIÓN 33
7.13.1 Registro de eventos 33
7.13.2 Protección de la información de registro 34
7.13.3 Sincronización de relojes 34
7.14 CONTROL DE SOFTWARE OPERACIONAL 34
7.14.1 Instalación de software en sistemas operativos 34
7.15 GESTIÓN DE LA VULNERABILIDAD TÉCNICA 35
7.15.1 Gestión de las vulnerabilidades técnicas 35
7.16 SEGURIDAD EN LAS COMUNICACIONES 35

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

ALCALDÍA MAYOR DE BOGOTÁ D.C.

7.16.1 Gestión de la seguridad en las redes 35
7.16.2 Transferencia de información 35
7.17 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 36
7.17.1 Requisitos de seguridad de los sistemas de información 36
7.17.2 Seguridad en los procesos de desarrollo y soporte 37
7.18 RELACIÓN CON LOS CONTRATISTAS (PROVEEDORES) 41
7.18.1 Seguridad de la información en las relaciones con los proveedores 41
7.19 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 42
7.20 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES 42
7.20.1 Identificación de la legislación aplicable y de los requisitos contractuales 42
7.20.2 Derechos de propiedad intelectual 42
7.20.3 Protección de registros 43
7.20.4 Privacidad y protección de información de datos personales 43
7.20.5 Reglamentación de controles criptográficos 43
7.21 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN 44
7.21.1 Revisión independiente de la seguridad de la información 44
7.21.2 Cumplimiento con las políticas y normas de seguridad 44
7.21.3 Revisión del cumplimiento técnico 44
7.21.4 Medidas a Adoptar en Caso de Incumplimiento 45
8. VIGENCIA 45
9. BIBLIOGRAFÍA 45

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

ALCALDÍA MAYOR DE BOGOTÁ D.C.

INTRODUCCIÓN

La Lotería de Bogotá adoptó el Sistema de Gestión de Seguridad de la Información-SGSI siguiendo las recomendaciones dispuestas en el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, como una herramienta habilitadora para gestionar la confidencialidad, integridad y disponibilidad de la información de forma eficiente, así mismo con lo relacionado con la administrando los riesgos, cumpliendo con la legislación vigente y, promoviendo una cultura de seguridad de la información en los servidores públicos, colaboradores y demás partes interesadas.

Con base en lo mencionado anteriormente, se busca proteger, preservar y administrar la integridad, confidencialidad, disponibilidad y autenticidad de la información de la entidad, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos de la entidad y en cumplimiento de los requisitos legales aplicables a la entidad, previniendo incidentes mediante la gestión de riesgos de seguridad y privacidad de la información, la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia a la ciudadanía en general.

En tal sentido, la lotería de Bogotá adopta el presente documento que contiene las políticas de seguridad de la información complementarias, como compromiso y responsabilidad que tiene la entidad con la confidencialidad, integridad y disponibilidad de la información, de acuerdo con lo establecido en el MSPI el cual toma como base la norma ISO/CEI 27001:2022 “Seguridad de la información, ciberseguridad y protección de privacidad – Sistemas de gestión de la seguridad de la información”; las cuales se implementan a partir de los planes, procedimientos y controles, asegurando la integración de los requisitos del sistema de seguridad en los procesos de la entidad, así como los recursos necesarios para su implementación y operatividad.

Este documento se complementa con el manual del SGSI de la lotería de Bogotá, la guía para identificación de activos de información, y demás herramientas que conforman el sistema.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

1. Política general del SGSI.

La LOTERÍA DE BOGOTÁ establece la política general de la seguridad de la información del SGSI, la cual es adecuada 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. Cuenta también con el compendio de políticas complementarías que se desarrollan en el presente documento.

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.

1.1 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.

2. OBJETIVO

Establecer las políticas de seguridad complementarias para preservar la confidencialidad, integridad, disponibilidad de los activos de información, mediante la gestión de los riesgos, que

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

permita además definir un marco de confianza a las partes interesadas en concordancia con la plataforma estratégica de la entidad.

2.1. Objetivos específicos

Las presente políticas de seguridad de la información están orientada al cumplimiento de los siguientes objetivos específicos:

- *Proteger la información de la lotería de Bogotá y de todos los grupos de interés en el marco de su gestión, salvaguardando su confidencialidad, integridad y disponibilidad a través del establecimiento de políticas para mitigar los riesgos que vulneren los activos de información.*
- *Fortalecer la cultura de seguridad de la información en los funcionarios, colaboradores, terceros, aprendices, practicantes y demás partes interesadas de la Lotería de Bogotá.*
- *Generar confianza en los ciudadanos, colaboradores y demás grupos de interés en las gestiones que se adelanten con la Lotería de Bogotá.*
- *Gestionar y mitigar los riesgos que se puedan presentar para proteger los activos de información de la Lotería de Bogotá. contra ataques, intrusiones, robo, accesos no autorizados y fuga de información que afecte a la imagen, los intereses y el buen nombre de la Lotería de Bogotá.*
- *Propender por un nivel apropiado de concientización, conocimientos y habilidades necesarios para minimizar la ocurrencia de incidentes de seguridad de la información.*

3. ALCANCE

Inicia con la descripción de los parámetros y disposiciones de las políticas del SGSI, continúa con las políticas específicas de seguridad y privacidad de la información y finaliza con la comunicación de estas.

Las políticas del SGSI aplican a todos los funcionarios, colaboradores, contratistas, proveedores y aquellas personas o terceros que, debido al cumplimiento de sus funciones u obligaciones, compartan, utilizan, recolectan, procesan, intercambien o consulten su información, así como los entes de control y entidades relacionadas que accedan, ya sea interna o externa a cualquier archivo de información, independiente de su ubicación. Así mismo, estas políticas aplican a toda la información creada, procesada, transmitida o resguardada por la Lotería de Bogotá, sin importar el medio, formato, presentación o lugar.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

4. NORMATIVIDAD (BASE LEGAL)

Que el artículo 15 de la Constitución Política de Colombia, consagra que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas". Que el artículo 209 ibidem, establece que, "la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley", y así mismo, en el artículo 269 impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

Que la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada parcialmente por el Decreto 1081 de 2015, tiene como objeto "desarrollar el derecho constitucional que tienen las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales" dicta, además las disposiciones generales para la protección de datos personales.

Que la 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", tiene por objeto "regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información".

Que el Decreto 1078 de 2015 Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, subrogado por el Decreto Nacional 1008 de 2018, en el artículo 2.2.9.1.1.3 señala que la Política de Gobierno Digital "se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998, 3° de la Ley 1437 de 2011, 2° y 3° de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2° de la Ley 1341 de 2009", y en particular los principios de innovación, competitividad, proactividad y seguridad de la información.

Que el Decreto Nacional No. 1083 de 2015, Decreto Único del Sector Función Pública, modificado por el Decreto Nacional No. 1499 de 2017, establece el MIPG, el cual integra los

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

sistemas de gestión de la calidad y de desarrollo administrativo creando un único sistema de gestión articulado con el sistema de control interno, el cual se actualiza y alinea con los mejores estándares internacionales.

Que en el CONPES 3854 de 2016 se establece la Política Nacional de Seguridad Digital en la República de Colombia, para realizar una gestión de riesgos de seguridad digital, con el fin de promover un entorno digital confiable y seguro, que maximice los beneficios económicos y sociales de los colombianos, impulsando la competitividad y productividad en todos los sectores de la economía.

Que teniendo en cuenta el MSPI, que conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permite garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que el artículo 2.2.9.1.2.1 del Decreto Nacional 1008 de 2018, define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes, que son las líneas de acción que orientan el desarrollo de su implementación, y habilitadores transversales, los cuales, son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que mediante el Decreto Distrital 591 de 2018 se adopta para el Distrito Capital el MIPG de que trata el Decreto Nacional 1083 de 2015, sustituido por el Decreto 1499 de 2017, como marco de referencia para el ajuste del diseño, la implementación y la mejora continua del Sistema Integrado de Gestión Distrital - SIGD, con el fin de fortalecer los mecanismos, métodos y procedimientos

5. DEFINICIONES

ACTIVO DE INFORMACIÓN: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

DATOS PERSONALES: Según la Ley 1581 de 2012, un dato personal se define como cualquier información que pueda asociarse a una o varias personas naturales determinadas o determinables. Una persona o individuo puede ser identificado directa o indirectamente a

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

través de su nombre, número de identificación, datos de ubicación, información laboral, entre otros.

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.

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: actividades coordinadas dentro de una organización, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

INFORMACIÓN PÚBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014

INFRAESTRUCTURA CRÍTICA CIBERNÉTICA NACIONAL: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado.

LINEAMIENTOS TI: Son reglas que especifican una acción o respuesta que se debe seguir en una situación determinada. En sí, son especificaciones técnicas que tienen una función instrumental que responden a cómo se implementa una política.

MEJORES PRÁCTICAS: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

MODELO DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN – MSPI: El Modelo de Seguridad y Privacidad de la Información entrega una guía para construir un Sistema de Gestión de Seguridad de la Información (SGSI), buscando generar una conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los activos de información de la entidad.

POLÍTICAS TI: Son directrices u orientaciones que debe generar la DTI y que indican la intención de la alta gerencia, con el propósito de establecer pautas para lograr los objetivos propuestos en la estrategia de TI. Son establecidas para que perduren a largo plazo y aplican a grupos grandes de áreas o personas dentro y, muchas veces, fuera de la organización (deben ser cumplidas por los contratistas y terceros y que por sus funciones deben tener acceso a la información y a su infraestructura).

PRIVACIDAD: se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

RIESGO DE SEGURIDAD DIGITAL: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.

SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

SEGURIDAD DIGITAL: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante la gestión del riesgo de seguridad digital; la implementación efectiva de medidas de ciberseguridad; y el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

SISTEMA DE GESTIÓN DE SEGURIDAD 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.

SOFTWARE: Son aquellos elementos informáticos, sobre los cuales la Secretaría Distrital de Gobierno, tiene el derecho de uso o de propiedad intelectual, que permiten que las labores de procesamiento de Información sirvan como herramienta de productividad y gestión. Están conformados entre otros por: A) Sistemas operativos. B) Software de ofimática, c) Software de desarrollo, D) Software comercial, E) Software de comunicaciones.

6. RESPONSABILIDAD Y AUTORIDAD

El máximo líder del SGSI es la Alta dirección, por medio del comité de gestión y desempeño, en donde estará la responsabilidad sobre el control, mejora y el seguimiento al cumplimiento de los elementos que conforman el SGSI articulados con el Modelo Integrado de Planeación y Gestión - MIPG, así como garantizar los recursos necesarios para su adecuado funcionamiento, en la Lotería de Bogotá.

Cabe mencionar que esta política se encuentra articulada con la política de administración de riesgos y las responsabilidades se enmarcan en las tres líneas de defensa base y la línea estratégica. Así mismo, se establece como máxima autoridad del Sistema de Gestión de Seguridad de la Información SGSI al Comité Institucional de Gestión y Desempeño quien es responsable de la orientación estratégica para la administración de los activos de información, la sostenibilidad y mejora del Sistema en la Entidad, como también garantizar los recursos necesarios para su adecuado funcionamiento, en la Lotería de Bogotá.

La política de seguridad de la información de la SDA está acorde con las mejores prácticas definidas en ISO 27001:2022 y el Modelo de Seguridad y Privacidad de la Información, por

tanto, todos los servidores públicos, colaboradores, contratistas, así como proveedores y usuarios en general, son responsables de su aplicación y tomarán las medidas aplicables para garantizar su cumplimiento. Respecto al tema de aprobaciones, todas las solicitudes hechas en temas que impacten a la Seguridad de la Información de la entidad y que necesiten aprobación, dado que pueden afectar la operación o la confidencialidad, disponibilidad e integridad de la información, deben ser solicitadas por los jefes de áreas y/o supervisores, por medio de la mesa de servicio.

6.1 Roles de seguridad de la información

Se deben tener en cuenta los roles establecidos en el manual de seguridad de la información de la Lotería de Bogotá sobre la información reservada, clasificada y pública, lo anterior con el fin de cumplir con la responsabilidad definida para cada rol; de esta manera se garantiza el adecuado manejo de la información, teniendo en cuenta los roles y responsabilidades asignadas según el cargo o actividades contractuales establecidas, además de las líneas de defensa establecidas en la política de administración de riesgos de la Lotería de Bogotá

Así mismo, los dueños y custodios que se identifican en inventarios de los activos de información deben tener asignado el rol adecuado, de acuerdo con el acceso que se tiene sobre cualquier activo. Dichos roles, deben estar asignados formalmente.

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

La secretaria Distrital de Ambiente establece las siguientes políticas de seguridad y privacidad de la información.

7.1 Seguridad de los recursos humanos

La Lotería de Bogotá aplica los lineamientos dados por la normatividad vigente y los procedimientos internos de selección y vinculación de personal, realizando las verificaciones necesarias para confirmar la veracidad de la información suministrada por el funcionario o la persona candidata a contratar.

Por medio del proceso de Gestión de Bienes y Servicios, se gestionan los contratos de proveedores y contratistas, es necesario tener en cuenta que, si en las actividades que se desarrollen en las fases contractuales, existe la posibilidad de tener manejo de información

sensible de la entidad, se deben aplicar los acuerdos de confidencialidad aprobados por la entidad.

El personal provisto por terceras partes que realicen labores para la Lotería de Bogotá debe aplicar y respetar las políticas de seguridad de la información y los acuerdos de confidencialidad, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

De igual forma, la entidad propenderá por la generación de la cultura de los funcionarios y contratistas de la Lotería de Bogotá con relación a la seguridad de la información, con el fin de reducir el riesgo, gestionar adecuadamente los activos de información y proteger las instalaciones, así como con los demás procedimientos y puntos de control generados en el marco del Sistema de Gestión de Seguridad de la Información – SGS.

7.1.1 Vinculación, desvinculación y cambio de cargo

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013 y la legislación aplicable con relación a la contratación pública, la vinculación laboral, retiro laboral y el cambio de cargo se llevarán a cabo siguiendo los procedimientos definidos para tal fin.

En la vinculación de los funcionarios o contratistas se deberá solicitar por talento humano, jefe de la oficina, líder de proceso o supervisor del contrato, la creación del usuario de red y de dominio; dicha solicitud deberá realizarse por petición al correo mesadeservicio@loteriadebogota.com. Cabe aclarar que, para los servidores públicos, se maneja desde Talento Humano y para contratistas, la Secretaría general.

7.1.2 Capacitación y entrenamiento en seguridad de la información

La LOTERÍA DE BOGOTÁ debe asegurar que todos los servidores, contratistas, visitantes y todos aquellos con acceso a la información y que tengan definidas responsabilidades de seguridad de la información sean competentes (en cuanto a capacitación formal y no formal) para desempeñar sus funciones u obligaciones.

La Oficina de Gestión Tecnológica e Innovación de la LOTERÍA DE BOGOTÁ solicitará a la Unidad de Talento Humano incluya en el Plan Institucional de Capacitación (PIC) como mínimo una capacitación al año sobre temas de seguridad de la información, para lo cual la Oficina de Gestión Tecnológica e Innovación la gestionará y desarrolla. La solicitud de Talento Humano o

supervisor del contrato enviado a mesadeservicio@loteriadebogota.com para la capacitación al servidor o contratista en los temas de seguridad., el cual hará parte del proceso de inducción de la LOTERÍA DE BOGOTÁ.

7.1.3 Procesos disciplinarios

Los procesos disciplinarios en la Lotería de Bogotá se tramitan conforme con lo dispuesto en la Ley 1952 de 2019 “Por el cual se expide el Código General Disciplinario”, por parte de la Oficina de Control Disciplinario Interno. En dicha Ley se establece, entre otras cosas, lo relacionado con la reserva procesal y las faltas disciplinarias relacionadas con la seguridad de la información a cargo de los servidores del Estado.

7.1.4 Intercambio de información

Cuando se desee intercambiar información pública clasificada o publica reservada se deberá clasificar de acuerdo con el caso:

- *Para los organismos de control y autoridades de supervisión se generará unacarta de Gerencia que implica la responsabilidad de la LOTERÍA DE BOGOTÁ, para la entrega de la información y el compromiso del ente que recibe con relación al manejo de dicha información en términos de seguridad y privacidad.*
- *Para los servidores y contratistas se encuentran en las cláusulas de confidencialidad de los contratos.*
- *Para terceros y partes interesadas se suscribirá un acuerdo de confidencialidad e intercambio de información y seguridad de la información entre las partes.*

7.2 Seguridad de la información en la gestión de contratos

La seguridad de la información debe ser parte integral en la entidad y se debe asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de los contratos. Esto aplicará a cualquier contrato, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los supervisores del contrato asegurar que se sigan las siguientes directrices:

- *Incluir cláusulas de seguridad de la información en el contrato.*

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

- *Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del contrato, para identificar los controles necesarios.*
- *Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del contrato.*

7.3 Dispositivos Móviles Y Teletrabajo O Trabajo En Casa

7.3.1 Dispositivos móviles

- *Se dispondrá de una red de invitados para la conexión de los equipos de visitantes a la Lotería, la cual permitirá la salida hacia Internet, pero no permitirá la conexión con equipos de cómputo o servidores de la LOTERÍA DE BOGOTÁ.*
- *Las estaciones de trabajo y equipos portátiles que son propiedad de la LOTERÍA DE BOGOTÁ cuentan con software licenciado y protección contra código malicioso.*
- *La LOTERÍA DE BOGOTÁ se reserva el derecho de monitorear y revisar los equipos de cómputo conectados a la red de la entidad.*
- *La LOTERÍA DE BOGOTÁ debe suministrar el antivirus para todos los equipos de la entidad.*

7.3.2 Teletrabajo o trabajo en casa

Cuando se requiera realizar labores de teletrabajo el jefe del área y/o dependencia a la cual pertenece el servidor o contratista, debe solicitar a la Oficina de Gestión Tecnológica e Innovación la configuración de una VPN petición a mesadeservicio@loteriadebogota.com, los servicios, ambientes y aplicativos a los cuales se requiere acceder. El servidor o contratista se debe comprometer a hacer un uso adecuado de la VPN.

7.4 GESTIÓN DE ACTIVOS

La Lotería de Bogotá establece métodos de protección para la propiedad legal del contenido de cualquier documento (físico, electrónico y digital) que se genere, obtenga, adquiera, transforme o controle durante el desarrollo de sus funciones.

La entidad se compromete mediante los líderes de los procesos y responsables, a identificar y proteger los activos de información, con el fin de garantizar su administración y control.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

Los activos de información serán identificados y/o actualizados cada vez que sea requerido por el líder de proceso asociado, con el apoyo técnico del Oficial de Seguridad de la Información, o quien haga sus veces. Determinando la clasificación de los activos de información de acuerdo con la criticidad, sensibilidad y reserva de esta, teniendo en cuenta la Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo con la naturaleza de la entidad. En caso de ser necesario, se podrá disponer del acompañamiento del proceso de gestión jurídica o un profesional en el área del conocimiento del Derecho que tenga la dependencia para su clasificación. La Gestión de activos se articula con la Política de administración de riesgos de la entidad y los procedimientos que de ella se deriven.

Así mismo, se debe tener en cuenta los siguientes lineamientos:

- *Los propietarios de los activos de información deben garantizar que los documentos que se clasifiquen con información parcialmente clasificada cuenten con una versión que contenga solo las partes que sí pueden ser publicadas.*
- *Se debe prever que los activos de información críticos se encuentren localizados en áreas/medios seguros y debidamente protegidos contra amenazas que puedan afectar su buen uso, disponibilidad y confidencialidad.*
- *Los activos de información críticos que sean de tipo digital deben estar protegidos con una contraseña.*
- *Se deben establecer controles o medidas acordes con la valoración de los activos de información y los riesgos asociados.*
- *Los colaboradores deben almacenar siempre la información digital de la entidad en las ubicaciones donde se esté respaldando la información.*
- *Se debe aplicar lo indicado en la guía para la identificación de activos de información de la Lotería de Bogotá.*

7.4.1 Inventario de activos

Los líderes de las oficinas, direcciones y unidades áreas responsables mantendrán actualizado el inventario de activos de la información, con base en la necesidad de cada proceso y de la entidad.

7.4.2 Asignación de activos

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

La asignación de los activos de información se realizará en coordinación con Unidad de Recursos Físicos y Oficina de Gestión Tecnológica e Innovación Recursos Físicos y Sistemas, de acuerdo con la solicitud del jefe inmediato o supervisor del contrato realizada a través del correo mesadeservicio@loteriadebogota.com.

7.4.3 Uso aceptable de los activos

La información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros), son activos de la entidad y se proporcionan a los servidores, contratistas y terceros autorizados, para cumplir con los propósitos de la LOTERÍA DE BOGOTÁ.
Los servidores, contratistas, proveedores y visitantes de la entidad deben reportar los eventos de seguridad de la información identificados al correo mesadeservicio@loteriadebogota.com.
Se deberá garantizar el diligenciamiento del Formato de Inventario Documental o el instrumento que haga sus veces, desde la producción de la información (Física y/o electrónica) independientemente de su soporte, lo cual permitirá el control seguimiento y cumplimiento durante del ciclo de vida de la información.

7.4.4 Devolución de activos

La devolución de activos se actualizará con la solicitud de almacén realizada al correo electrónico mesadeservicio@loteríadebogotá.com.
La devolución de equipos de cómputo o activos cuando se finalizan contratos o se presente retiro definitivo de la entidad o traslado de funciones, se hará por medio de la solicitud por parte de talento humano a través de correo electrónico mesadeservicio@loteríadebogotá.com.

7.4.5 Uso de equipos de cómputo

Está prohibido que personal ajeno a la Oficina de Gestión Tecnológica e Innovación, destape o retire partes de los equipos de cómputo que pertenecen al inventario de la LOTERÍA DE BOGOTÁ.
La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad de la Oficina de Gestión Tecnológica e Innovación, por tanto, se debe realizar

una solicitud al correo mesadeservicio@loteriadebogota.com para la realización de estas actividades.

Los equipos de cómputo no podrán ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario o contratista al que le fue asignado, sin previo aviso la Oficina de Gestión Tecnológica e Innovación y Almacén. Debe respetarse y no modificarse la configuración de hardware y software establecida por la Oficina de Gestión Tecnológica e Innovación. Se restringe el acceso de medios extraíbles (USB, discos externos, CD, DVD, entre otros) para almacenamiento de información institucional en todas las estaciones de trabajo de la entidad, salvo las autorizadas explícitamente por la gerencia de la entidad.

Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de la LOTERÍA DE BOGOTÁ, está prohibida y dará lugar a los procesos disciplinarios y/o legales correspondientes establecidos en la presente politica.

Durante la permanencia en las instalaciones de la LOTERÍA DE BOGOTÁ, los equipos de cómputo externos deben estar conectados únicamente a la red de datos Wifi corporativa configurada por la Oficina de Gestión Tecnológica e Innovación, en caso de requerir acceso a la red LAN o cableada, deben hacer la solicitud a través de la mesa de servicio, cualquier otro tipo de acceso no está autorizado y dará lugar a los procesos disciplinarios y/o legales correspondientes.

Los equipos de cómputo (CPU), servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados (tapa naranja), el monitor debe conectarse a la toma de corriente normal (toma blanca).

La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de la LOTERÍA DE BOGOTÁ y que no son propiedad de la entidad, serán responsabilidad única y exclusiva de sus propietarios. La LOTERÍA DE BOGOTÁ, no será responsable por estos equipos en ningún caso.

7.4.6 Uso de internet

Está prohibido conectar cualquier dispositivo en modo Access Point para acceder a Internet, dentro de la red WAN de la entidad. Queda prohibido a todos los funcionarios y contratistas acceder a cualquier página o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de la LOTERÍA DE BOGOTÁ tales como violencia, terrorismo, grupos

al margen de la ley, discriminación, entre otras. Se prohíbe el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal, institucional o que conlleven a la comisión de algún delito.

Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red de la LOTERÍA DE BOGOTÁ, no se permite el envío o descarga de información masiva como música, videos y/o software no autorizado.

Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta (correo, directorio activo y demás aplicaciones institucionales).

Todas las actividades realizadas en los sistemas de información de la LOTERÍA DE BOGOTÁ podrán ser monitoreadas con el fin de preservar la seguridad informática de la entidad.

Los usuarios no deben intentar burlar o evadir los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la entidad y de la ley y serán sancionadas, que en caso de funcionarios se realiza con base en la Ley 1952 de 2019 “Por el cual se expide el Código General Disciplinario”; para el caso de contratistas y terceros, se debe evaluar su cumplimiento desde la supervisión del contrato y escalar con los entes competentes.

7.4.7 Uso del correo institucional

La entidad proveerá a todos los funcionarios y contratistas un correo electrónico institucional en el dominio loteriadebogota.com, de acuerdo con las funciones realizadas y a la capacidad de cuentas disponibles apropiadas en la LOTERÍA DE BOGOTÁ.

- *La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus credenciales de acceso y el buzón asociado al correo de la entidad.*
- *El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la LOTERÍA DE BOGOTÁ, es decir, que debe ser usado para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo asignadas.*
- *Teniendo en cuenta que el correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo y no una herramienta de difusión masiva de información, no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político,*

religioso o racial, amenazas, estafas, virus o código malicioso. Acciones de esta naturaleza se consideran violatorias de las políticas de la entidad y de la ley y serán sancionadas de acuerdo con la Ley 1952 de 2019 "Por el cual se expide el Código General Disciplinario". Para el caso de contratistas y terceros, se debe evaluar su cumplimiento desde la supervisión del contrato y escalar con los entes competentes.

- *El servidor de correo bloqueará archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos.*
- *Bajo ningún motivo se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas e información de la LOTERÍA DE BOGOTÁ.*
- *En casos de generar password o clave de forma automática, el usuario debe cambiarla en el momento en que acceda a la plataforma de correo electrónico.*
- *La información contenida en el buzón es de completa responsabilidad del usuario, en caso de eliminación accidental de correos electrónicos, inclusive de la papelera, se puede pedir apoyo mediante la mesa de servicio. Teniendo en cuenta que no se asegura una recuperación de los correos al 100%, y depende de la funcionalidad y disponibilidad de la plataforma de correo que se tenga contratada por la entidad.*
- *Si por cualquier razón el usuario sospecha o sabe que la seguridad de su cuenta se ve comprometida de cualquier forma, debe cambiar su contraseña e informar al oficial de seguridad de la información.*
- *En caso de recibir correos sospechosos, en los que no se tenga conocimiento o relación de los temas a tratar, además con adjuntos; debe abstenerse de abrirlos y descargar los archivos adjuntos. Si el remitente del correo es una entidad pública, se debe verificar con la entidad la autenticidad de este, antes de realizar cualquier gestión. y debe notificar a Seguridad de la Información, por medio de la mesa de servicios, para adelantar el análisis respectivo.*

No está permitido abrir, usar o revisar la cuenta de correo electrónico de otro usuario como si fuera propia o suplantándolo. Solamente se podrá acceder al correo electrónico para consulta de otro usuario bajo las siguientes excepciones:

- *Los colaboradores con nivel Directivo podrán realizar solicitudes relacionadas con el correo electrónico de colaboradores que están bajo su coordinación o supervisión.*

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

- *Que el servidor público que se ausente por enfermedad o vacaciones y la entidad tenga la imperante necesidad de acceder a la información que se encuentre en los dispositivos o correos asignados al colaborador. Para el caso de los contratistas, por ausencia, suspensión o terminación del contrato, el supervisor del contrato podrá acceder a dicha información; cabe mencionar que el acceso es solo para consulta y no para comunicaciones en nombre de la persona a la que se le ha asignado la cuenta.*
- *Que el colaborador y la entidad rompan estrepitosamente la relación laboral o contractual y LOTERÍA DE BOGOTÁ requiera acceso a la información que se encontraba en poder del colaborador.*
- *Cuando existan sospechas de espionaje corporativo, de algún acto de corrupción, soborno, lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva, incidente de seguridad de la información o en general, de alguna actividad delictiva por parte de algún colaborador que pudiera afectar los intereses de la LOTERÍA DE BOGOTÁ.*
- *Para evitar el sabotaje, la modificación o eliminación de la información que se encuentre en poder de algún colaborador, en caso de un eventual conflicto o terminación de la relación laboral o contractual con la entidad.*

El usuario debe notificar correos sospechosos a través de la mesa de servicio GLPI o mediante el correo mesadeservicio@loteriadebogota.com, estos correos no deben ser reenviados a ningún usuario, no se deben abrir enlaces, ni abrir los archivos adjuntos que contengan.
El servidor que entre en periodo de vacaciones o ausencia de algún tipo debe redireccionar su correo electrónico a su jefe inmediato o supervisor del contrato (caso de contratistas) o a quien asignen sus funciones, de no hacerlo la entidad podrá bloquear dicha cuenta.
El uso incorrecto del correo electrónico institucional podrá dar lugar a eventuales sanciones disciplinarias de acuerdo con la Ley 1952 de 2019 “Por el cual se expide el Código General Disciplinario”.

7.5 Gestión de medios removibles (unidades de almacenamiento)

La LOTERÍA DE BOGOTÁ promoverá el uso de carpetas compartidas en lugar de medios removibles (USB, discos externos, CD/DVD, entre otros) para el intercambio de información al interior de la entidad.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

Las unidades de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se administrarán mediante directorio activo y quien requiera hacer uso de estas unidades debe solicitar la activación la Oficina de Gestión Tecnológica e Innovación, previa autorización del jefe de direcciones, oficinas y unidades ~~unidad~~, indicando el tiempo por el cual se requiere la activación.

- *Las personas que requieran los medios removibles habilitados de forma permanente deben tener una autorización por el jefe de dependencia y/o área.*
- *La empresa de vigilancia de la entidad controlará el ingreso y salida de los equipos de cómputo de la entidad.*
- *Los medios removibles en los que se almacene información catalogada como información pública clasificada e información pública reservada deben estar cifrados.*

Si ya no se requiere el contenido de un medio reusable, se debe remover de forma que la información no se pueda recuperar, esta actividad será responsabilidad de la Oficina de Gestión Tecnológica e Innovación.

7.5.1 Almacenamiento En la Nube y carpetas compartidas

El almacenamiento en la nube es un servicio que proporciona un lugar de almacenamiento para los archivos, así como la posibilidad de crear documentos de texto, hojas de cálculo, presentaciones, formularios y carpetas. Además, permite compartirlos con otros usuarios. Todas las cuentas de usuario tienen acceso a un espacio personal de almacenamiento en la nube y un espacio compartido con todos los usuarios de una dependencia.

- *El contenido de las carpetas en la nube y de las carpetas compartidas, debe albergar documentos finales o aprobados. Las carpetas de las cuentas personales pueden almacenar documentos de trabajo o documentos finalizados. Por ninguna razón se debe transferir a las carpetas información personal excepto si está es soporte de una actuación pública o parte de la gestión contractual con la Lotería de Bogotá.*
- *Los usuarios son responsables de todas las actividades realizadas con sus cuentas de espacio en la nube.*
- *No se debe facilitar y ofrecer acceso a la propia cuenta a personas no autorizadas por la Lotería de Bogotá o su representante legal.*
- *La estructura de las carpetas y archivos de la unidad de cada dependencia estará a cargo de la persona que delegue el jefe de cada dependencia.*

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

- *Los espacios asignados para cada dependencia, solo debe tener registrada información institucional.*
- *Los administradores de cada dependencia deben velar por mantener actualizada y organizada la información de cada carpeta, de ser necesario eliminar las versiones borrador o las que no se consideren finales.*
- *Así mismo, se deben asignar permisos sobre carpetas compartidas a grupos de usuarios.*
- *Es responsabilidad de cada usuario el manejo adecuado y la información que se almacena en los espacios asignados.*

7.6 Clasificación de la información

En atención a los requisitos de la norma NTC-ISO/IEC 27001:2013, la Ley 1712 de 2014 y el Decreto 103 de 2015, la LOTERÍA DE BOGOTÁ clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con las actividades de Control de Documentos de la LOTERÍA DE BOGOTÁ.

7.6.1 Disposición de los medios

Los medios que contienen información confidencial se deben disponer en concordancia con lo establecido en la ley 1581, TITULO II PRINCIPIOS RECTORES, articulo 4, literales: a), f), g) y h), en tal sentido la disposición de la información de que trata el presente numeral, se realizará teniendo en cuenta la legalidad del procedimiento, con la debida autorización del dueño de la información y/o por las personas que determine la ley, acatando y siguiendo las medidas técnicas (destrucción, borrado de datos o el procedimiento establecido en la política de tratamiento de datos de la Lotería de Bogotá) y administrativas que garanticen la seguridad y reserva de la información.

En caso de requerirse, transportar información de Backups que contengan información reservada o clasificada, en medios físicos como discos o cintas, se deben cifrar antes de ser entregados a la empresa transportadora. Lo anterior atendiendo a los principios de los literales: b) Principio de finalidad y d) Principio de veracidad y calidad, antes de ser entregados a la empresa transportadora

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

La información almacenada en medios magnéticos con obsolescencia tecnológica tendrá que ser migrada a medios con tecnología actual, antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos.

7.6.2 Transferencia de medios físicos

Para la transferencia de medios físicos se deben seguir las directrices y orientaciones establecidas en el proceso de gestión documental, y el instrumento archivístico pertinente, desarrollado para realizar el Control de Documentos de la LOTERÍA DE BOGOTÁ, así como los documentos relacionados

7.7 CONTROL DE ACCESO

La Lotería de Bogotá gestiona el control de acceso de todos los servidores públicos, funcionarios, contratistas, proveedores y usuarios a las redes, aplicaciones, información física, sistemas de información, e instalaciones de procesamiento de información.

Para la Lotería de Bogotá es prioritario definir el personal que debe tener acceso sobre la información que considera es sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas, únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la Entidad debe salvaguardar y custodiar su información de forma adecuada, y más cuando es información categorizada como sensible o tener un carácter confidencial. Así mismo, es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de esta.

La administración de la plataforma tecnológica es responsabilidad de la Oficina de Gestión Tecnológica e Innovación, y controla los accesos de los usuarios a través del directorio activo, así como los sistemas de información de la Entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso pertinentes a dichos recursos.

7.7.1 Política de control de acceso a los sistemas de información.

La Oficina de Gestión Tecnológica e Innovación controlará el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

Lo que necesita conocer: solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).
Lo que necesita usar: solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.
Establecer y verificar que los datos de acceso a los sistemas están compuestos por un nombre de usuario, una contraseña y que sean únicos para cada servidor público, colaborador o tercero.
En caso de retiro, terminación, jubilación, suspensión, cesión o cambio de cualquier servidor público, colaborador o tercero, se deberá deshabilitar o actualizar los privilegios en los sistemas a los que el usuario estaba autorizado, lo anterior siempre con el soporte documental que respalde la acción y previa comunicación de la dependencia solicitante y a la cual pertenece el usuario y la novedad.

7.7.2 Acceso a redes y a servicios en red

Ningún servidor público o contratista podrá compartir archivos o carpetas de un equipo de cómputo a otro sin la respectiva autorización de la Oficina de Gestión Tecnológica e Innovación y del jefe inmediato o supervisor.
El acceso a redes Wifi se controla con autenticación por contraseña utilizando el protocolo WPA2-PSK o el portal cautivo.
La Oficina de Gestión Tecnológica e Innovación proporciona un servicio de conectividad a todos los servidores, contratistas, proveedores y visitantes de la entidad para la navegación en internet, la cual es controlada mediante perfiles de navegación.
La conexión remota a la red de área local de La LOTERÍA DE BOGOTÁ debe ser realizada a través de una conexión VPN segura o mediante conexión de acceso remoto, suministrada por la Oficina de Gestión Tecnológica e Innovación, previa autorización del jefe de unidad o líder de proceso quien será el encargado de realizar la solicitud formal a la Oficina de Gestión Tecnológica e Innovación.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

7.7.3 Gestión de acceso de usuarios

El acceso a usuarios, la gestión de derechos de acceso privilegiado, la gestión de información de autenticación secreta, retiro o ajuste a los derechos de acceso se realizan de acuerdo con la solicitud previamente enviada por la Unidad de Talento Humano, o jefes de direcciones, unidades y oficinas o líderes de procesos al correo mesadeservicio@loteríadebogotá.com.

7.7.4 Uso de Información de autenticación secreta (Responsabilidades de los Usuarios)

Cada usuario es responsable de mantener a salvo la contraseña de ingreso al equipo. Adicionalmente, los usuarios autorizados a acceder a los sistemas de información de la LOTERÍA DE BOGOTÁ son responsables de la seguridad de las contraseñas y cuentas de usuario. Cabe resaltar que las contraseñas son únicas e intransferibles.

- *No se deberá guardar o escribir las contraseñas en papeles físicos o documentos de texto como bloc de notas, Word o las notas de Windows.*
- *La contraseña escogida para el acceso a cada uno de los sistemas de información de la LOTERÍA DE BOGOTÁ debe:*
- *Ser diferente para cada aplicación o sistema de información con excepción de aquellos sistemas que se autentiquen contra el directorio activo.*
- *No debe contener características personales o de los parientes tales como nombres, apellidos, fechas de cumpleaños o alguna otra fecha importante.*
- *No debe contener palabras de diccionario. Las palabras en idioma inglés y español son las primeras utilizadas por los atacantes.*

Las contraseñas se deben establecer teniendo en cuenta los siguientes parámetros: Deben contener mayúsculas, minúsculas, números, caracteres especiales y mínimo ocho (8) caracteres. Las contraseñas deben ser cambiadas cada cuarenta y cinco (45) días. Para ello, las aplicaciones controladas mediante el directorio activo al igual que el correo electrónico, exigirán el cambio automático de las contraseñas con la periodicidad mencionada. Las contraseñas del Sistema ERP (SICOF) y Misional deben ser actualizadas por el usuario.
Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.

Para desbloquear la clave de acceso a los diferentes sistemas de información, el usuario debe realizar la solicitud ante la mesa de servicio a través del correo mesadeservicio@loteriadebogota.com.

7.7.5 Control de acceso a sistemas y aplicaciones

El control de acceso a sistemas y aplicaciones se establece de acuerdo con el rol del usuario y sus funciones en la entidad, el jefe inmediato debe enviar por correo la solicitud a través de la mesa de servicio - mesadeservicio@loteriadebogota.com.

Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas (root, SYS, SYSADMIN, cuenta de administrador de Windows, entre otras) deben ser cambiadas anualmente o cada vez que expire el tiempo.

La Oficina de Gestión Tecnológica e Innovación debe cambiar las contraseñas por defecto (y donde sea posible, los usuarios por defecto) de las aplicaciones y servicios utilizados por la LOTERÍA DE BOGOTÁ.

El uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones, no están permitidos para fines diferentes a las actividades propias de la Oficina de Gestión Tecnológica e Innovación.

7.8 CONTROLES CRIPTOGRÁFICOS

La Oficina de Gestión Tecnológica e Innovación debe determinar los algoritmos criptográficos y protocolos autorizados para su uso en la entidad y configurar los sistemas para permitir únicamente aquellos algoritmos autorizados, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifrados débiles tales como DES, RC3, RC4 y protocolos débiles tales como SSLv2 y SSLv3. Se debe considerar en su lugar el uso de algoritmos tales como AES (cifrado simétrico), RSA (cifrado asimétrico) y los protocolos SSL/TLS 1.2 o 1.3 y tamaños de cifrado de 168 o 256 bits (cifrado simétrico) y 2048 bits (cifrado asimétrico) preferiblemente en el caso de ser requeridos.

Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

La administración de tokens bancarios, tokens para acceso a sistemas de información de entes de control y firmas digitales, estarán a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus funciones y/u obligaciones.

Los tokens bancarios y tokens de acceso sistemas de información de entes de control y firmas digitales, deben estar almacenados bajo llave cuando no los están utilizando o cuando se van a retirar de sus puestos de trabajo.

7.9 SEGURIDAD FÍSICA Y DEL ENTORNO

7.9.1 Áreas seguras

La LOTERÍA DE BOGOTÁ cuenta con los siguientes controles para prevenir el acceso no autorizado a las instalaciones de la entidad.

- *Sistema de acceso biométrico en la entrada, para servidores y/o contratistas.*
- *El personal de vigilancia, son los encargados de validar el ingreso de visitantes con el área la Unidad, oficina y dirección correspondiente, en caso de ingresar equipos deben quedar registrados en la minuta respectiva.*
- *Cámaras de seguridad en los pasillos de la LOTERÍA DE BOGOTÁ, monitoreadas todo el tiempo desde la recepción de la entidad. Las grabaciones deben permanecer por el tiempo que la capacidad de almacenamiento de la entidad lo permita.*

El Centro de Cómputo de la LOTERÍA DE BOGOTÁ cuenta con sistema de detección y extinción de incendios, aire acondicionado, sistema de alimentación ininterrumpida (UPS) y corriente regulada.

Las áreas de la LOTERÍA DE BOGOTÁ están delimitadas por una barrera física y el ingreso debe hacerse a través de cualquiera de las dos puertas de acceso controlada por cerraduras.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

El Centro de Cómputo debe contar con mecanismos que garanticen que cumplen los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

Todo acceso al Centro de Cómputo de la LOTERÍA DE BOGOTÁ se registra por medio de una bitácora de acceso, en donde se deben registrar los accesos y tiempo de permanencia y actividad a realizar.

7.9.2 Ubicación y protección de los equipos

El Centro de Cómputo está ubicado en la Oficina de Gestión Tecnológica e Innovación, de forma tal que personas no autorizadas no puedan ingresar y tener acceso físico. Este acceso es controlado por los funcionarios de la Oficina de Gestión Tecnológica e Innovación.

7.9.3 Servicios de suministro

La entidad cuenta con aire acondicionado, un sistema de alimentación no interrumpida (UPS), que asegura el tiempo necesario para que entre en funcionamiento la planta eléctrica que tiene el edificio, también se tiene un canal dedicado para el acceso a internet con su respectivo canal de backup.
La planta eléctrica es la encargada de suministrar energía de respaldo en caso de interrupciones del suministro eléctrico principal, permitiendo que los equipos de computación funcionen de manera ininterrumpida y evita pérdida de datos o daños en los equipos debido a cortes de energía.

7.9.4 Seguridad del cableado

El cableado del Centro de Cómputo de la entidad debe cumplir con la normas y buenas prácticas de cableado estructurado (como por ejemplo la ISO/IEC 11801 o ANSI/TIA-568-C.1) y estar debidamente certificado.

7.9.5 Mantenimiento de equipos

La Oficina de Gestión Tecnológica e Innovación establece, ejecuta (mantenimiento correctivo), subcontrata (mantenimiento preventivo) y hace seguimiento a los planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

7.9.6 Seguridad de equipos y activos fuera de las instalaciones

La salida de equipos de cómputo fijos y de escritorio de la entidad se debe controlar mediante memorando o correo electrónico, autorizada por el jefe de la unidad de recursos físicos y/o del Almacén. Esta política aplica para todos los funcionarios y/o contratistas, excepto para el (la) gerente, subgerente y secretario general. Para el caso de equipos portátiles, en portería los usuarios deben reportar el ingreso y salida de los equipos, y se deja el registro en la bitácora de vigilancia.

Los medios removibles que son retirados de las instalaciones de la entidad con Backup deben ser debidamente cifrados por la Oficina de Gestión Tecnológica e Innovación.

Los servidores y contratistas que retiren equipos o medios removibles de las instalaciones de la entidad deben seguir las siguientes directrices:

- *En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.*
- *Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.*

En caso de pérdida o robo de un equipo de la entidad, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al Unidad de Recursos Físicos, al responsable del Almacén y al responsable de la Oficina de Gestión Tecnológica e Innovación para que se inicie el trámite interno correspondiente. Así mismo, se debe reportar al Oficial de Protección de Datos para que reporte el incidente ante la Superintendencia de Industria y Comercio SIC según lo dispuesto en el procedimiento para tal fin.

7.9.7 Disposición segura o reutilización de equipos

Cuando una estación de trabajo, equipo portátil o medio removible vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la' información de la entidad que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

o sobreescritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma.
Para el caso de las licencias que se encuentran en físico se destruyen y se deja evidencia y testigos del procedimiento realizado.

7.9.8 Política de equipo desatendido, escritorio y pantalla limpios

Los servidores públicos funcionarios y contratistas de la LOTERÍA DE BOGOTÁ deben conservar su escritorio físico libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento.
Los computadores mostrarán por defecto el fondo y protector de pantalla que la LOTERÍA DE BOGOTÁ defina, incluyendo publicidad institucional o temas corporativos.; estos no podrán ser modificados por ningún usuario y deben permanecer activos.
Los funcionarios y contratistas de la LOTERÍA DE BOGOTÁ deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo.
Se prohíbe el almacenamiento de información personal en los computadores y servidores de la LOTERÍA DE BOGOTÁ.
El escritorio lógico debe estar libre de información pública clasificada e información pública reservada.

7.10 SEGURIDAD DE LAS OPERACIONES

7.10.1 Documentación de procedimientos operativos

Se debe contar con procedimientos o guías documentadas para las actividades operativas asociadas con las instalaciones de software y procesamiento de información, los cuales deben definir las restricciones que se aplican para estas actividades.

7.10.2 Control de cambios

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

Los cambios en los procesos de negocio serán gestionados por el Comité Institucional de Gestión y Desempeño (CIGYD).
Los cambios en la documentación de los procesos se deben realizar siguiendo las actividades que soportan el Control de Documentos.
Los cambios en los sistemas de información se realizan de acuerdo con la solicitud de realizadas por el servidor a través de la mesa de servicio mesadeservicio@loteriadebogota.com.

7.10.3 Gestión de capacidad

La entidad gestiona la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones que serán tomadas en la Oficina de Gestión Tecnológica e Innovación.

7.10.4 Separación de los ambientes

La entidad cuenta con ambientes de desarrollo y producción separados por máquinas virtuales.
La entidad controla el acceso al ambiente de desarrollo de la misma forma que controla el acceso al ambiente de producción, siguiendo las directrices de la política de control de acceso.

7.11 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- *Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de la entidad contra códigos maliciosos.*
- *Los contratistas y servidores públicos que hagan uso de equipos portátiles personales deben contar con un software antivirus licenciado.*
- *El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos de la LOTERÍA DE BOGOTÁ conectados a la red deben tener el antivirus instalado y activo.*

El único servicio de antivirus autorizado para las estaciones de trabajo y los equipos portátiles de los funcionarios de la LOTERÍA DE BOGOTÁ es el asignado directamente por la Oficina de Gestión Tecnológica e Innovación, el cual cumple con todos los requisitos técnicos y de seguridad requeridos.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.
El usuario NO debe instalar o emplear programas no autorizados para manejo de antivirus.
Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa antivirus.
El programa antivirus debe ser instalado única y exclusivamente por la Oficina de Gestión Tecnológica e Innovación, en los servidores, estaciones de trabajo y equipos de cómputo de los Servidores Públicos funcionarios y contratistas de la LOTERÍA DE BOGOTÁ.
Es deber de los usuarios informar a la Oficina de Gestión Tecnológica e Innovación en caso de que el antivirus no se encuentre activo o este desactualizado.

7.12 COPIAS DE RESPALDO

La entidad debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello la Oficina de Gestión Tecnológica e Innovación cuenta con actividades para realizar la Gestión de Copias de Seguridad.
La Oficina de Gestión Tecnológica e Innovación establecerá las políticas y estándares de copias de seguridad para los sistemas de información y bases de datos.
Las copias de respaldo se guardarán únicamente con el objetivo de restaurar información cuando por situaciones como borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o equipos de cómputo, o por requerimientos legales, sea necesario recuperarla.
Los funcionarios y contratistas son responsables de almacenar la información que requiera copias de respaldo, en las carpetas compartidas asignadas por la Oficina de Gestión Tecnológica e Innovación a cada una de las áreas de la LOTERÍA DE BOGOTÁ, dado que la información que se encuentra almacenada en ubicaciones diferentes no será respaldada.

7.13 REGISTRO Y SUPERVISIÓN

7.13.1 Registro de eventos

Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de la entidad, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

7.13.2 Protección de la información de registro

La Oficina de Gestión Tecnológica e Innovación con el fin de proteger la información de registro de modificación por parte de usuarios no autorizados, administradores u operadores de los sistemas de información, implementará mecanismos para generar logs en sus aplicaciones, para tener control y trazabilidad.

7.13.3 Sincronización de relojes

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la LOTERÍA DE BOGOTÁ deberán estar sincronizados por el servidor de dominio.

7.14 CONTROL DE SOFTWARE OPERACIONAL

7.14.1 Instalación de software en sistemas operativos

El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de la Oficina de Gestión Tecnológica e Innovación. Por lo tanto, a cualquier otro servidor público o contratista no le es permitido realizar esta labor.

Para la instalación de software se tendrán en cuenta las siguientes directrices por la Oficina de Gestión Tecnológica e Innovación y únicamente es esta Área la que podrá hacer cualquier instalación:

- *El software propietario debe contar con su respectiva licencia y en el caso del software libre debe estar permitido el uso comercial.*
- *El instalador debe ser descargado de la página oficial del fabricante.*
- *Debe verificarse la integridad del archivo por medio de la comprobación de códigos hash (siempre que el fabricante proporcione esta información).*
- *Ningún usuario se encuentra autorizado para instalar aplicaciones o software en los equipos de Cómputo de la LOTERÍA DE BOGOTÁ.*

- *Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de los nuevos sistemas de información o mejoras a sistemas de información existentes, antes de su puesta en marcha.*
- *Todos los sistemas nuevos y mejorados deben estar completamente soportados por una documentación suficientemente amplia y actualizada, y no deben ser puestos en el ambiente de producción sin contar con la documentación disponible.*

7.15 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

7.15.1 Gestión de las vulnerabilidades técnicas

La Oficina de Gestión Tecnológica e Innovación, es responsable de verificar de manera periódica (al menos semestralmente) la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la entidad.

Se debe generar y ejecutar por lo menos una vez al año un plan de análisis de vulnerabilidades y/o hacking ético para las plataformas críticas de la LOTERÍA DE BOGOTÁ, cuya viabilidad técnica y de administración lo permita.

7.16 SEGURIDAD EN LAS COMUNICACIONES

7.16.1 Gestión de la seguridad en las redes

La Oficina de Gestión Tecnológica e Innovación debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de las redes, los servicios en red y la información por allí transmitida.

La Oficina de Gestión Tecnológica e Innovación define e implementa los mecanismos de separación de las redes de la LOTERÍA DE BOGOTÁ con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de acceso interno)

El acceso remoto a las redes de la entidad se controla mediante conexiones VPN.

7.16.2 Transferencia de información

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

La entidad incluye una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial. En este acuerdo quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se firmarán antes de permitir el acceso o uso de dicha información.

Los funcionarios públicos y contratistas deben seguir las indicaciones de gestión documental para la transferencia de información, siguiendo los parámetros de la clasificación de la información de acuerdo con las tablas de retención documental - TRD de la LOTERÍA DE BOGOTÁ y con la Política de Tratamiento de Datos de la entidad.

7.17 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

7.17.1 Requisitos de seguridad de los sistemas de información

La Oficina de Gestión Tecnológica e Innovación define los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en la entidad. Para ello, deben tener en cuenta:

- *El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. Por ejemplo,la implementación de segundos factores de autenticación y un sistema de gestiónde contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar de nuevo su uso.*
- *Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.*
- *Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada, el envío de información por canales cifrados.*
- *Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas y uso de firmas digitales.*
- *Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.*
- *La necesidad de exigir la implementación de metodologías de desarrollo seguro.*

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

- *Todos los desarrollos o adquisición de software de terceros deben ser gestionados por la Oficina de Gestión Tecnológica e Innovación con el fin verificar requisitos técnicos y seguridad de la información.*

7.17.2 Seguridad en los procesos de desarrollo y soporte

7.17.2.1 Política de desarrollo seguro

La Lotería de Bogotá debe garantizar un ambiente de desarrollo seguro durante la ejecución de los proyectos, arquitecturas, software o sistemas, estableciendo metodologías que incluya requisitos de seguridad en cada una de las fases del proyecto, acuerdos de soporte y niveles de servicio a terceros, y separación física y virtual en los ambientes de operación, todo a través de técnicas de programación seguras. Así mismo, cada sistema de información deberá contar con sus manuales de uso y técnicos disponibles de acuerdo con los niveles de protección de la información dados para estos datos, así como la arquitectura del software.

Los administradores de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de funcionamiento establecidos antes del paso a producción de los sistemas. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica.

Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

En todos los desarrollos que se adelanten en la Lotería de Bogotá se deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.

Los aplicativos desarrollados proporcionarán la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

Se debe garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

Se debe garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

La privacidad, confidencialidad e integridad del activo de información, con base en el nivel al que pertenezca y el nivel de evaluación de riesgo, deberá ser salvaguardada a través de la aplicación de:

- *Cifrado de datos clasificados como reserva: Los datos en tránsito entre diferentes sistemas y el almacenamiento de esta información se deben cifrar con un algoritmo criptográfico. Usar HTTPS para aplicaciones web.*
- *Control de acceso: Mecanismos de autenticación por usuario y contraseña siguiendo la Política de control de acceso a la información establecida.*
- *Registro: Registrar eventos que evidencien las acciones realizadas con el fin de tener un registro de auditoría de las acciones que realiza el usuario.*
- *Validar la integridad de los datos: Implementar opciones que permitan validar la integridad de los datos almacenados y/o transmitidos dependiendo de su criticidad.*

Las funcionalidades y archivos que no sean necesarios para los aplicativos se removerán, previo a la puesta en producción, además se debe prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

Además, no se debe permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

7.17.2.2 Cambios en sistemas, plataforma tecnológica o paquetes de software

Los cambios en sistemas deben llevarse a cabo de acuerdo con el procedimiento Gestión del Cambio PRO340-472-2.

7.17.2.3 Principios de desarrollo seguro

La Oficina de Gestión Tecnológica e Innovación debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos. Se debe contar con un protocolo para revisar los desarrollos que entregan los diferentes contratistas (Proveedores), para garantizar la calidad de los entregables y el cumplimiento de los requerimientos hechos.

Los principios de desarrollo establecidos se deben aplicar con base en el protocolo 02. PRO340-243-10 DESARROLLO DE APLICACIONES, en donde se definen las actividades para asegurar

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

que se está contribuyendo a mejorar los estándares de seguridad dentro del proceso de desarrollo y asegurar que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Los datos de configuración del sistema como, por ejemplo: contraseñas, direcciones IP, datos de conexión a bases de datos y otros parámetros de configuración deben quedar almacenadas en archivos o bases de datos cifradas. Está prohibida la inclusión de estos parámetros en el código fuente.

7.17.2.4 Ambiente de desarrollo seguro

La Oficina de Gestión Tecnológica e Innovación aplicará los mismos controles aplicados al ambiente de producción en el ambiente de pruebas, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

La Oficina de Gestión Tecnológica e Innovación debe asegurar que las migraciones entre los ambientes de pruebas y producción han sido aprobadas y son exitosas, de acuerdo con las actividades para gestionar cambios de seguridad de la información.

La Oficina de Gestión Tecnológica e Innovación debe contar con sistemas de control de versiones para administrar los cambios en los sistemas de información desarrollados al interior de la entidad.

7.17.2.5 Desarrollo contratado externamente

La Oficina de Gestión Tecnológica e Innovación debe asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

Las áreas y/o dependencias deben exigir el suministro de evidencia que se realizaron pruebas de seguridad al software desarrollado por terceros.

Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

Las áreas y/o dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

Las áreas y/o dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes y regulaciones aplicables.
Las áreas y/o dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la entidad a realizar auditorías durante el desarrollo del contrato.
Cuando se contrata un desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por la entidad. Adicionalmente, se debe acordar la entrega de manual(es) técnico(s), que describa(n) la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manual(es) funcional(es), que describa(n) las funcionalidades de cada una de las opciones del menú de la aplicación. Así mismo, se deben incluir cláusulas de confidencialidad.

7.17.2.6 Pruebas de seguridad de sistemas

Se debe contar tanto para desarrollos internos como externos con la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

7.17.2.7 Pruebas de aceptación de sistemas

Se deben realizar pruebas de aceptación del software, independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable).
En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido los defectos relacionados con la seguridad.
De ser posible, las pruebas de aceptación se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente de la entidad, y que las pruebas son confiables.

7.17.2.8 Datos de prueba

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

La Oficina de Gestión Tecnológica e Innovación debe certificar que la información a ser entregada a los desarrolladores (tanto internos como externos) para sus pruebas será enmascarada o que los datos sensibles serán eliminados con el fin de no revelar información confidencial de los ambientes de producción y, por ende, dar cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

7.18 RELACIÓN CON LOS CONTRATISTAS (PROVEEDORES)

7.18.1 Seguridad de la información en las relaciones con los proveedores

7.18.1.1 Política de seguridad de la Información para las relaciones con Contratistas (proveedores)

La LOTERÍA DE BOGOTÁ, por medio de los supervisores establecerá mecanismos de control en sus relaciones con contratistas (proveedores), con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que se cumpla con las políticas de la entidad. Esta actividad, dependerá de la naturaleza y particularidad del servicio prestado.

7.18.1.2 Tratamiento de la seguridad dentro de los acuerdos con Contratistas (proveedores)

Los supervisores de contratos se asegurarán de comunicar las políticas y procedimientos a los proveedores y/o contratistas.

Se deben incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información:

- *Cláusula de confidencialidad.*
- *Cláusula de protección de datos personales.*
- *Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).*
- *Cumplimiento de las políticas de seguridad de la información de la LOTERÍA DE BOGOTÁ.*

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

- *Acciones para tomar en caso de incumplimiento de las políticas de seguridad de la información.*
- *Reporte de eventos de seguridad de la información a través de la mesadeservicio@loteriadebogota.com.*
- *Cláusula de seguimiento y revisión de los servicios prestados por los proveedores y/o contratistas para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan.*
- *Responsabilidades de los proveedores incluidos en la cadena de suministro, tales como, soporte técnico y garantía.*

Los supervisores de contratos deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos, y monitoreando la aparición de nuevos riesgos.

Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Oficina de Gestión Tecnológica e Innovación a través de la mesa de servicios mesadeservicio@loteriadebogota.com.

7.19 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.

7.20 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

7.20.1 Identificación de la legislación aplicable y de los requisitos contractuales

La Secretaría General y el Oficial de Seguridad o quien haga sus veces, deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la entidad que están relacionados con seguridad de información. Para ello, se pueden apoyar en el Comité Institucional de Gestión y Desempeño (CIGD).

7.20.2 Derechos de propiedad intelectual

La Oficina de Gestión Tecnológica e Innovación realizará revisiones periódicas (al menos semestralmente), con el fin de asegurar que todo el software que se ejecute en la entidad esté

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados para el desarrollo de sus funciones.

Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, La Oficina de Gestión Tecnológica e Innovación podrá distribuir un número de copias de software bajo una licencia otorgada.

Los supervisores de contratos deben asegurarse de incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

7.20.3 Protección de registros

La LOTERÍA DE BOGOTÁ se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de confidencialidad, disponibilidad e integridad, siguiendo las directrices de los activos de información.

7.20.4 Privacidad y protección de información de datos personales

La LOTERÍA DE BOGOTÁ, quien será responsable del tratamiento de los Datos Personales, tal y como este término se define en la Ley 1581 de 2012, respeta la privacidad de cada uno de los terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de dicha información. Por lo tanto, la entidad implementará los controles necesarios para su protección y en ningún momento divulgará esta información a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la ley lo permita. Además, se debe cumplir con lo establecido en la Política para el tratamiento de datos personales aprobada por la entidad.

7.20.5 Reglamentación de controles criptográficos

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

La LOTERÍA DE BOGOTÁ, se regirá por la Ley 527 de 1999 (acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y otras disposiciones) y sus decretos reglamentarios, según se requiera.

7.21 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

7.21.1 Revisión independiente de la seguridad de la información

La Oficina de Control Interno realizará auditorías internas de revisión al Modelo de Seguridad y Privacidad de la Información, siguiendo las directrices del procedimiento de Auditorías Internas al Sistema Integrado de Gestión. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la entidad para gestionar la seguridad de la información.

7.21.2 Cumplimiento con las políticas y normas de seguridad

Los jefes de unidad y/o dependencia deben revisar con regularidad (al menos una vez por año) el cumplimiento de las políticas y procedimientos de seguridad de la información dentro de su área de responsabilidad. La Oficina de Gestión Tecnológica e Innovación, lidera el apoyo y asesoramiento para su eficiente cumplimiento.

7.21.3 Revisión del cumplimiento técnico

La Oficina de Gestión Tecnológica e Innovación debe coordinar la revisión periódica (La periodicidad se establece con base en la necesidad y recursos con los que cuente la entidad) de los sistemas de información utilizados en la LOTERÍA DE BOGOTÁ, para determinar el cumplimiento en términos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se hará revisión cada vez.

7.21.4 Medidas a Adoptar en Caso de Incumplimiento

El incumplimiento de una o más políticas descritas en este documento, está sujeto a las sanciones disciplinarias, fiscales y penales según se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo o en comisión, de acuerdo con la Ley 1952 de 2019, la Ley 906 de 2004 y la Ley 1273 de 2009.

8. VIGENCIA

Las presentes políticas entrarán en vigencia a partir de la fecha de aprobación.

9. BIBLIOGRAFÍA

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

www.loteriadebogota.com - cliente@loteriadebogota.com
PBX (57) 1 335 1535 - Carrera 32A # 26 -14

POLÍTICAS COMPLEMENTARIAS DE LA INFORMACIÓN		
CODIGO:	POL340-648-1	**VERSIÓN: 1**
ELABORÓ	**REVISÓ**	**APROBÓ**
LUIS ALEJANDRO RUIZ	YOLANDA PATRICIA GALLEGO GALVIS	Comité De Gestión Y Desempeño
Contratista	Profesional Especializado OGTI	

REGISTRO DE MODIFICACIONES		
VERSIÓN	**FECHA**	**DESCRIPCIÓN MODIFICACIÓN**
01	21-04-2025	Versión inicial