Política de Seguridad de la Información

Lotería de Medellín

2026

Aprobado el 24 de agosto de 2026, mediante Acta N°8 del Comité Institucional de Gestión y Desempeño para la política de seguridad.

1. Introducción

La información es un activo esencial para las actividades de las empresas, y en consecuencia necesita una protección adecuada. La seguridad de la información tiene como fin la protección de la información y de los sistemas que la soportan, frente a un gran número y variedad de amenazas y vulnerabilidades.

En el presente documento se describen las Políticas, Normas de Seguridad de la Información y lineamientos de Ciberseguridad definidos por la Lotería de Medellín. Para su elaboración se toman como base las directrices establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) del Gobierno Nacional, el cual se fundamenta a su vez en el estándar internacional **ISO/IEC 27001:2022**, la Ley 1581 de 2012 (Protección de Datos Personales) y la Guía para la Gestión Integral del Riesgo en Entidades Públicas."

2. Justificación

Las entidades públicas están obligadas a disponer de un conjunto de políticas de seguridad de la información que sirva como carta de navegación en lo relacionado con los controles técnicos, físicos y organizacionales que se deben implementar para garantizar altos niveles de seguridad, privacidad y resiliencia de la información gestionada a través de sus sistemas.

Teniendo en cuenta que la información transaccional y operativa es el activo más crítico para la prestación de los servicios, la ciberseguridad es una prioridad ineludible para la Lotería de Medellín. Por tanto, es responsabilidad de todos sus miembros e instancias de gobierno velar por su cumplimiento, de tal manera que se adopte una postura proactiva frente a las amenazas digitales y se eviten prácticas que comprometan la operación institucional.

3. Alcance

Las directrices establecidas en la presente Política de Seguridad de la Información son de obligatorio y estricto cumplimiento para todos los funcionarios públicos, trabajadores oficiales, contratistas, consultores, practicantes, proveedores de servicios tecnológicos y cualquier tercero que tenga acceso, administre, procese o almacene activos de información propiedad de la Lotería de Medellín.

El alcance de esta política abarca:

- Todos los procesos estratégicos, misionales (con especial criticidad en la gestión de sorteos, comercialización y validación de premios), de apoyo y de evaluación y control definidos en la entidad.
- Toda la infraestructura tecnológica e instalaciones físicas.
- Los entornos de procesamiento remoto, modalidades de teletrabajo y los servicios tecnológicos alojados en la nube (Cloud Computing).
- La cadena de suministro de Tecnologías de la Información y las Comunicaciones (TIC).

4. Objetivos De Seguridad De La Información

4.1. Objetivo General:

Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los activos de información y de la infraestructura tecnológica de la Lotería de Medellín. Esto se logrará gestionando proactivamente los riesgos de ciberseguridad para asegurar la continuidad ininterrumpida de los procesos misionales, la transparencia de los sorteos y la protección de los datos de nuestros grupos de valor, en estricto cumplimiento del marco legal y normativo vigente (MSPI, Ley 1581, MIPG).

4.2. Objetivos Específicos:

- Identificar y Proteger: Clasificar y salvaguardar la información institucional, protegiendo especialmente los datos personales de los clientes (Habeas Data) y la integridad de los aplicativos de sorteos, mitigando riesgos de fuga de información (DLP) y accesos no autorizados.

- Detectar proactivamente: Implementar capacidades de monitoreo continuo sobre la infraestructura tecnológica para identificar de manera temprana vulnerabilidades, amenazas cibernéticas y comportamientos anómalos.

- Responder y Recuperar (Resiliencia Operativa): Asegurar la preparación de las TIC para resistir incidentes de ciberseguridad, garantizando una contención oportuna y la recuperación de los servicios críticos de la Lotería en los tiempos de tolerancia establecidos (RTO/RPO).

- Cumplimiento y Cultura Digital: Fomentar una cultura sólida de ciberseguridad y uso seguro de la información entre los colaboradores y terceros, asegurando el cumplimiento de los lineamientos del MINTIC, Coljuegos y los entes de control.

5. Público objetivo

La presente Política de Seguridad de la Información está dirigida a las siguientes partes interesadas, quienes asumen una responsabilidad compartida en la protección de los activos institucionales y la resiliencia operativa de la Lotería de Medellín:

- Alta Dirección y Líderes de Proceso: Responsables de ejercer el liderazgo, aprobar los lineamientos estratégicos, asignar los recursos necesarios y promover una cultura de seguridad digital desde la gerencia hacia toda la entidad.

- Funcionarios, Trabajadores Oficiales, Contratistas y Practicantes: Responsables de conocer, comprender y aplicar de manera estricta los controles de seguridad en sus actividades diarias. Tienen el deber de proteger la información a su cargo y reportar de manera inmediata cualquier evento, incidente o sospecha de ciberataque.

- Proveedores y Cadena de Suministro de TIC: Terceros, fabricantes, consultores y proveedores de servicios (incluyendo aquellos que administran infraestructura física, software de sorteos o servicios en la nube). Están obligados a dar cumplimiento a esta política a través de acuerdos de confidencialidad (NDA), controles de acceso y Acuerdos de Nivel de Servicio (SLA) en materia de ciberseguridad.

- Clientes, Apostadores, Distribuidores y Entes de Control (MinTIC, Coljuegos, Contraloría): Actúan como los principales grupos de valor y beneficiarios de esta política. Hacia ellos, la Lotería de Medellín garantiza la máxima transparencia en la operación, la integridad de los sorteos y la protección irrestricta de sus datos personales (Habeas Data).

6. Marco Legal

La presente Política de Seguridad de la Información se enmarca en el cumplimiento de la normatividad vigente en materia de seguridad de la información, protección de datos personales, transparencia y lineamientos técnicos nacionales e internacionales. A continuación, se relacionan las principales disposiciones aplicables:

Norma / Referencia	Descripción
Constitución Política de Colombia (1991)	Marco normativo superior. Establece los principios y derechos fundamentales aplicables a la protección de la información, el derecho a la intimidad (Art. 15) y el acceso a documentos públicos (Art. 74).
Leyes 23 de 1982 y 594 de 2000	Ley de Derechos de Autor (protección de software y licenciamiento) y Ley General de Archivos (gestión documental y conservación de la información institucional).
Ley 1273 de 2009	Tipifica los delitos informáticos en Colombia y protege de manera integral la información, los datos y los sistemas que los procesan.
Ley 1581 de 2012 y Decreto 1377 de 2013	Ley General de Protección de Datos Personales (Habeas Data) y su decreto reglamentario. Establecen los lineamientos para la recolección, almacenamiento y uso de datos personales.
Ley 1712 de 2014 y Decreto 103 de 2015	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y su decreto reglamentario. Obliga a la clasificación y publicación proactiva de la información.
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC. Incorpora los lineamientos de la Política de Gobierno Digital.
Modelo de Seguridad y Privacidad de la Información (MSPI - MinTIC)	Lineamientos nacionales y guías vigentes del Ministerio TIC para la implementación de la seguridad y privacidad en entidades públicas, articulado con el MIPG.
Decreto 2106 de 2019	Establece disposiciones relacionadas con la simplificación de trámites e incluye aspectos asociados al uso de medios electrónicos y el manejo de datos personales.
Documento CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital. Establece la hoja de ruta para la ciberseguridad y resiliencia en el Estado colombiano.
Circular Externa 007 de 2022 (SIC)	Lineamientos de la Superintendencia de Industria y Comercio sobre el reporte obligatorio y la gestión de incidentes de seguridad que afecten bases de datos personales.
Guías y Lineamientos SIC (2023)	Documentos técnicos y guías de buenas prácticas emitidas por la SIC para el tratamiento seguro de datos personales.
Guía DAFP / MinTIC (Versión 7 - 2025)	Guía para la Gestión Integral del Riesgo en Entidades Públicas. Define la metodología para tratar los riesgos de seguridad digital integrados al mapa institucional.

Norma / Referencia	Descripción
Norma Técnica NTC 6767:2024	Norma Técnica Colombiana fundamental para la entidad, que establece los requisitos de seguridad y calidad para los procesos de pre-sorteo y sorteo de juegos de suerte y azar.
Norma ISO/IEC 27001:2022	Estándar internacional actualizado que define los requisitos para establecer, implementar, mantener y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información (SGSI).

7. Definiciones

- Activo: Cualquier elemento físico o intangible que tiene valor para la entidad.
- Activo de Información: Cualquier información o elemento relacionado con el tratamiento de esta (software, hardware, personas, bases de datos, etc.) que tenga valor para la organización y deba ser protegido
- Ciberdefensa: Conjunto de políticas, acciones y buenas prácticas de orden gubernamental para garantizar un acceso seguro al ciberespacio por parte de los ciudadanos y proteger la infraestructura crítica del Estado.
- Ciberresiliencia : Capacidad de la Lotería de Medellín para anticipar, resistir, recuperarse y adaptarse rápidamente frente a ciberataques o condiciones adversas en sus sistemas tecnológicos.
- Ciberseguridad: Conjunto de tecnologías, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos (ciberespacio) frente a ataques, daños o accesos no autorizados.
- Confidencialidad: Atributo de la Seguridad de la Información que garantiza que los datos solo estén disponibles y sean revelados a individuos, entidades o procesos autorizados.
- Disponibilidad: Atributo de la Seguridad de la Información que garantiza que los datos y sistemas estén accesibles y utilizables de manera oportuna por las personas autorizadas.
- Evaluación de riesgos de Seguridad de Información: Proceso estructurado de identificación, análisis y valoración de riesgos que puedan afectar la confidencialidad, integridad o disponibilidad.
- Identidad y Credenciales de Acceso (Antes "Id de usuario"): [Actualizado] Elemento lógico (usuario) que, junto con un factor de autenticación (contraseña, token, biometría), permite verificar la identidad de una persona para otorgarle acceso a la red o aplicativos.

- Incidente de Seguridad de la Información: Evento o serie de eventos de seguridad inesperados que tienen una alta probabilidad de comprometer las operaciones de la entidad y amenazar sus activos de información.
- Informática Forense: Aplicación de técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos digitales (evidencia) que sean válidos dentro de un proceso legal o investigativo.
- Información pública clasificada: Información en poder de la entidad que pertenece al ámbito propio, particular y privado de una persona natural o jurídica (ej. datos de apostadores). Su acceso podrá ser negado bajo los amparos del artículo 18 de la Ley 1712 de 2014.
- Información pública reservada: Información en poder de la entidad que es exceptuada de acceso a la ciudadanía por riesgo de daño a intereses públicos, cumpliendo los requisitos de la Ley 1712 de 2014.
- Integridad: Atributo de la seguridad que busca mantener los datos exactos y completos, libres de modificaciones o alteraciones no autorizadas.
- Inteligencia de Amenazas / Threat Intelligence: Información recolectada, analizada y contextualizada sobre ataques y amenazas cibernéticas (IOCs) que permite a la entidad tomar decisiones proactivas de defensa.
- ISO/IEC 27001: Estándar internacional cuya tercera edición fue publicada en 2022. Establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).
- ISO/IEC 27002: Código de buenas prácticas (versión 2022) que proporciona un conjunto de 93 controles de referencia (Organizacionales, Personas, Físicos y Tecnológicos) para mitigar riesgos.
- Mabe: Nombre del servicio de Mesa de Ayuda de la Oficina de las TIC de la Lotería de Medellín.
- Modelo de Seguridad y Privacidad de la Información (MSPI): Lineamiento del MinTIC, integrado al MIPG, basado en la ISO 27001 y la Ley 1581, que guía a las entidades públicas en la protección de su información.
- No repudio: Propiedad que permite probar la participación de las partes en una comunicación o transacción. Previene que un emisor o receptor niegue haber enviado o recibido un mensaje (Vital para la venta de lotería online).
- Plan de Continuidad del Negocio (BCP): Plan logístico y tecnológico orientado a garantizar que las operaciones críticas de la entidad se mantengan o recuperen rápidamente tras un evento disruptivo.
- Prevención de Fuga de Datos / DLP: Medidas tecnológicas diseñadas para detectar y bloquear la extracción o transferencia no autorizada de información confidencial.

- Política de escritorio y pantalla limpia: Lineamientos para garantizar que los usuarios protejan la información física y digital en su espacio de trabajo cuando se ausentan.
- Presorteo: Actividades preparatorias y validaciones técnicas o procedimentales previas a la ejecución del sorteo oficial.
- Ransomware: Tipo de software malicioso crítico que cifra (secuestra) los datos o sistemas de la entidad, exigiendo un pago a cambio de liberar la información.
- Registro inmutable: Bitácora protegida que garantiza la integridad y la no alteración de los logs o datos (mediante criptografía), fundamental para la transparencia del sorteo y auditorías.
- Riesgo de Seguridad de la Información: Posibilidad de que una amenaza explote una vulnerabilidad, causando un impacto negativo en los activos de la entidad.
- Seguridad de la información: Conjunto de políticas, procedimientos y prácticas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información en todos sus formatos.
- SIEM y SOC: El SIEM (Gestor de Eventos e Información de Seguridad) es la herramienta tecnológica que centraliza los logs, y el SOC (Centro de Operaciones de Seguridad) es el equipo que monitorea y responde a las alertas generadas.
- Sistema de prevención de intrusos (IPS/WAF): Tecnologías de seguridad que monitorean el tráfico de red y las aplicaciones web para bloquear ataques en tiempo real.
- Software malicioso (Malware) / Virus: Código informático diseñado para infiltrarse, alterar, dañar o extraer información de los sistemas sin el consentimiento del usuario.
- Sorteo: Actividad auditable que genera un resultado aleatorio oficial para la Lotería de Medellín.
- Trazabilidad: Capacidad de reconstruir cronológicamente (quién, qué, cuándo y dónde) las acciones en un sistema, vital para investigar incidentes y auditar el proceso de sorteo.
- Veedor / Auditor externo: Persona o entidad independiente designada para validar el correcto y transparente desarrollo de las fases de sorteo y presorteo.
- Vulnerabilidad: Debilidad de un activo, proceso o control que puede ser explotada por una amenaza cibernética.

8. Vigencia, Revisión Y Divulgación

8.1. Vigencia y Revisión:

La presente Política de Seguridad de la Información entrará en vigor a partir de la fecha de su aprobación por parte del Gerente y el Comité Institucional de Gestión y Desempeño de la Lotería de Medellín.

Para garantizar su idoneidad, adecuación y eficacia continua, esta política será revisada y actualizada por lo menos una vez al año, o de forma extraordinaria cuando se presenten cambios significativos en la infraestructura tecnológica, en la legislación nacional (MinTIC/SIC) o tras la ocurrencia de un incidente crítico de ciberseguridad.

8.2. Divulgación y Comunicación:

El Jefe de las TICs y la Oficina de Comunicaciones serán responsables de garantizar que este documento sea comunicado, entendido y aplicado de forma transversal. La política deberá ser divulgada mediante los canales oficiales a todos los funcionarios, trabajadores oficiales y contratistas. Asimismo, estará disponible como información pública para terceros, proveedores tecnológicos y grupos de valor a través del sitio web oficial de la Lotería de Medellín.

9. Principios MSPI y Directrices Específicas De Seguridad

Las responsabilidades frente a la Seguridad, Ciberseguridad y Privacidad de la Información serán definidas, compartidas, publicadas y aceptadas formalmente por cada uno de los servidores públicos, proveedores, contratistas y terceros. Para dar cumplimiento al Modelo de Seguridad y Privacidad de la Información (MSPI), la Lotería de Medellín establece los siguientes principios de obligatorio cumplimiento:

- Cumplimiento Legal y Privacidad desde el Diseño: La entidad se compromete con el estricto cumplimiento de la normatividad colombiana sobre protección de datos, en especial la Ley 1581 de 2012 (Habeas Data) y la Ley 1712 de 2014 (Transparencia). Todo nuevo proyecto tecnológico o modificación en los aplicativos de sorteos deberá contemplar la privacidad y seguridad desde su concepción.
- Protección en la Cadena de Suministro y Servicios en la Nube (Cloud): Se protegerá la información generada, procesada o resguardada por los procesos de negocio frente a los riesgos derivados de accesos otorgados a terceros, acuerdos de nivel de servicio (SLA), esquemas de *outsourcing* o almacenamiento en infraestructuras de nube. Se exigirán auditorías y controles equivalentes a los internos.
- Prevención de Fuga y Extracción de Información (DLP): La información es un activo crítico de la Lotería de Medellín. Por lo tanto, queda estrictamente prohibida su extracción, copia o transferencia hacia medios no autorizados o canales personales. Se implementarán controles tecnológicos (DLP) y de monitoreo continuo para

bloquear cualquier exfiltración que atente contra la confidencialidad, integridad y disponibilidad del negocio.

- Disposición y Destrucción Segura de Medios: Se contará con un procedimiento técnico riguroso para la baja y disposición final de los equipos informáticos y medios de almacenamiento (discos duros, USB, servidores). Se garantizará la eliminación segura de los datos mediante técnicas de borrado seguro (sobrescritura o borrado criptográfico) o destrucción física certificada, impidiendo cualquier intento de recuperación forense de la información institucional.
- Transferencia Segura de la Información: Todo intercambio de información física o electrónica, tanto al interior de la entidad como con entes externos (Coljuegos, MinTIC, distribuidores), se realizará a través de canales oficiales, cifrados y con mecanismos que garanticen la trazabilidad y el *No Repudio* de la transacción.

Principios orientadores:

En concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI), la norma ISO/IEC 27001:2022 y la NTC 6767:2024, la Lotería de Medellín adopta como principios rectores de su gestión de Seguridad, Ciberseguridad y Privacidad de la Información:

- ***Confidencialidad**:* proteger la información de accesos no autorizados.
- ***Integridad**:* asegurar que la información no sea alterada de manera indebida.
- ***Disponibilidad**:* garantizar que la información esté accesible cuando sea requerida.
- ***Ciberresiliencia***: Mantener la capacidad de anticipar, resistir, responder y recuperarse rápidamente ante incidentes cibernéticos o fallas tecnológicas, garantizando la continuidad de la operación institucional.
- ***Trazabilidad y no repudio*:** Asegurar que toda transacción, acceso o modificación en los sistemas de información (incluyendo el presorteo y sorteo) deje un registro auditable e inmutable que no pueda ser negado por sus autores.
- ***Legalidad y cumplimiento**:* respetar la normativa aplicable.
- ***Imparcialidad**:* garantizar que los procesos de presorteo y sorteo estén libres de influencias internas o externas que afecten su objetividad.
- ***Transparencia**:* asegurar que los presorteos y sorteo sean verificables, auditables y confiables para la ciudadanía.

10. Roles y Responsabilidades en Seguridad y Privacidad de la Información

La Lotería de Medellín establece los siguientes roles y responsabilidades para garantizar la correcta implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI):

- **Alta Dirección (Gerencia):** Aprobar la política, asignar los recursos financieros, técnicos y humanos necesarios, definir los lineamientos estratégicos y promover activamente una cultura institucional de ciberseguridad y resiliencia.
- **Comité Institucional de Gestión y Desempeño:** Actuar como la máxima instancia de revisión del SGSI. Supervisar la eficacia de los controles, aprobar el tratamiento de riesgos críticos y coordinar acciones de mejora continua a nivel gerencial.
- **Jefe de las TIC:** Liderar el diseño, implementación y evaluación del SGSI. Es el encargado de articular el cumplimiento del MSPI, reportar el desempeño de la seguridad a la Alta Dirección y coordinar la respuesta ante incidentes críticos de ciberseguridad.
- **Oficina TIC:** Implementar y administrar los controles tecnológicos y de ciberdefensa. Es responsable del monitoreo continuo (SOC/SIEM), la gestión de vulnerabilidades, las copias de respaldo y la preparación de la infraestructura para la continuidad del negocio (DRP).
- **Área Jurídica:** Asesorar sobre el cumplimiento normativo en materia de protección de datos personales (Habeas Data) y transparencia. Garantizar que los contratos con proveedores y terceros incluyan cláusulas estrictas de confidencialidad (NDA) y Acuerdos de Nivel de Servicio (SLA) en seguridad.
- **Responsables del proceso de Presorteo y Sorteo:** Velar por que todas las actividades operativas del core de negocio se realicen bajo los principios de imparcialidad, transparencia y trazabilidad, garantizando la custodia, registro inmutable y protección de la información según la norma NTC 6767.
- **Servidores públicos, contratistas y terceros:** Conocer, firmar y cumplir irrestrictamente las políticas, directrices y acuerdos de confidencialidad. Son responsables del uso aceptable de los activos asignados y de reportar de forma inmediata a la Mesa de Ayuda (Mabe) cualquier sospecha, incidente o debilidad que amenace la seguridad digital.

11. Gestión de Riesgos de Seguridad, Ciberseguridad y Privacidad de la Información

La Lotería de Medellín adoptará un enfoque preventivo, proactivo y basado en riesgos para proteger la información y asegurar la ciberresiliencia de sus procesos críticos. Para ello:

- **Articulación Institucional (MIPG):** La valoración y tratamiento de los riesgos digitales se realizará en estricto cumplimiento de la **Guía para la Gestión Integral del Riesgo en Entidades Públicas (Versión 7 - 2025)**, garantizando que los riesgos de ciberseguridad y privacidad formen parte del mapa de riesgos institucional.

- **Evaluación Continua:** Se identificarán, analizarán y evaluarán periódicamente los riesgos, contemplando escenarios de amenazas cibernéticas modernas (ej. *Ransomware*, ataques de denegación de servicio, exfiltración de bases de datos) que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad.
- **Tratamiento Técnico:** Se aplicarán medidas de tratamiento apoyadas en los controles del Anexo A de la norma **ISO/IEC 27001:2022**, alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Protección Core del Negocio:** Se priorizarán con tratamiento de máxima criticidad aquellos riesgos que puedan impactar la imparcialidad, transparencia y confiabilidad de los procesos de **presorteo y sorteo**, aplicando controles específicos ineludibles para asegurar su correcta ejecución según la norma NTC 6767:2024.
- **Inteligencia de Amenazas:** El análisis de riesgos no será estático. Se retroalimentará constantemente del monitoreo tecnológico (SOC/SIEM) y de la Inteligencia de Amenazas (*Threat Intelligence*) para anticipar vulnerabilidades y tomar decisiones oportunas de mitigación.

12. Gestión y Respuesta a Incidentes de Seguridad, Ciberseguridad y Privacidad de la Información

La Lotería de Medellín implementará un proceso formal para la detección, reporte, análisis, tratamiento y cierre de incidentes de seguridad y privacidad de la información, garantizando la trazabilidad y el aprendizaje organizacional. Este proceso operará bajo las siguientes directrices, alineadas con la norma ISO/IEC 27001:2022 y el MSPI:

- **Monitoreo y Detección Temprana (SOC/SIEM):** La entidad contará con capacidades tecnológicas de monitoreo continuo sobre su infraestructura y aplicativos web (ej. WAF), permitiendo la detección temprana de eventos anómalos, ataques cibernéticos y posibles fugas de información.
- **Reporte Obligatorio:** Todos los directivos, servidores, contratistas y terceros deberán reportar de inmediato a la Mesa de Ayuda de TI cualquier sospecha o incidente de seguridad que afecte la confidencialidad, integridad, disponibilidad o trazabilidad de la información.
- **Respuesta, Contención y Ciberresiliencia:** Se definirán roles, responsabilidades y tiempos de respuesta (SLA) para atender los incidentes de manera eficaz, garantizando la contención rápida de las amenazas y la activación oportuna de los planes de Continuidad del Negocio (BCP) cuando la operación se vea comprometida.
- **Protección del Sorteo y Cadena de Custodia:** Los incidentes relacionados con los procesos de sorteo y presorteo recibirán atención prioritaria, asegurando la transparencia, legalidad y confianza pública en los resultados. En caso de incidentes críticos, se aplicarán procedimientos de recolección de evidencia digital (Informática Forense) garantizando su cadena de custodia y no repudio.
- **Notificación Legal y a Autoridades:** En caso de materializarse una brecha de seguridad que comprometa bases de datos con información personal, la entidad realizará el reporte obligatorio ante la Superintendencia de Industria y Comercio (SIC) conforme a la Circular Externa 007 de 2022. Asimismo, los ciberataques críticos serán notificados a los equipos de respuesta a emergencias cibernéticas del Estado (ColCERT / CSIRT Nacional).

13. Documento de la política de seguridad y privacidad de la Información

El presente documento incluye las siguientes características de obligatorio cumplimiento:

- Se exponen claramente los objetivos del MSPI y el propósito de este documento.
- Se expone el alcance de las políticas y directrices aquí descritas.
- Las políticas de Seguridad, Ciberseguridad y Privacidad están directamente alineadas con los objetivos estratégicos de la Lotería de Medellín.
- Estas políticas son aprobadas formalmente por el Comité Institucional de Gestión y Desempeño y establecen un compromiso indelegable con la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).
- Las políticas deben ser socializadas permanentemente para garantizar que tanto los usuarios internos como terceros externos las conozcan, las comprendan y las pongan en práctica.
- El documento contiene una descripción clara del significado de Seguridad de la Información, Ciberseguridad, Privacidad y Ciberresiliencia.
- Se definen los roles, responsabilidades y responsables en la construcción y gestión del MSPI.
- Se definen los procesos y mecanismos generales para el manejo de incidentes, situaciones y eventos excepcionales de seguridad.

14. Organización de la seguridad de la información

Roles y responsabilidades para la seguridad de la información: La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Lotería de Medellín, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

La coordinación de la implementación del MSPI está a cargo de la Oficina de las TIC, pero cada una de las áreas de la Lotería de Medellín deben identificar, documentar, implementar, evaluar y controlar los aspectos de la política que afecten cada uno de sus procesos.

14.1. Separación de deberes y tareas:

Tanto en las responsabilidades de gestión de la seguridad, como en los roles de los aplicativos, se debe procurar una estricta separación de deberes. Esto busca prevenir modificaciones no autorizadas o fraudes, garantizando que las operaciones críticas (como

el sorteo, validación de premios y asignación de permisos) no sean ejecutadas y auditadas por una sola persona.

14.2. Contacto con las autoridades

Se debe contar con un procedimiento y responsabilidades definidas para la denuncia de potenciales violaciones, tanto si se trata de ciberataques, incidentes técnicos o violaciones de confidencialidad. Esto incluye el contacto oportuno con autoridades competentes como el Centro Cibernético Policial (Fiscalía), el CSIRT Nacional / ColCERT y la Superintendencia de Industria y Comercio (SIC).

14.3. Contacto con grupos de interés e Inteligencia de Amenazas

La Oficina de las TIC deben mantener actualizado el conocimiento y las experticias técnicas. Esto implica disponer de suscripciones a boletines, foros y fuentes de Inteligencia de Amenazas (Threat Intelligence) de carácter internacional y nacional que faciliten la prevención de ataques y la mejora continua.

14.4. Seguridad de la información en la gestión de proyectos

Todos los proyectos, nuevos desarrollos o adquisiciones tecnológicas deben cumplir con la presente política para su definición e implementación. Se exigirá la aplicación de los principios de Seguridad y Privacidad desde el Diseño y por Defecto.

15. Seguridad de los Recursos Humanos

15.1. Selección e investigación de antecedentes: La Dirección de Talento Humano debe realizar todas las verificaciones de los antecedentes penales, fiscales y disciplinarios de los candidatos que se postulan a un cargo en la Lotería de Medellín.

15.2. Términos y condiciones del empleo: El contrato de trabajo de los funcionarios de la Lotería de Medellín contiene una cláusula en donde se determinan las normas esenciales para el acceso a los sistemas de información, el uso de claves, la propiedad de la información en los sistemas de información, la propiedad de los desarrollos y mejoras intelectuales realizados durante la ejecución de dicho contrato.

Los acuerdos contractuales o de confidencialidad definidos por la entidad, reflejan los compromisos de protección y buen uso de la información y sus responsabilidades en cuanto a la seguridad de la información.

15.3. Responsabilidades de la dirección

Todos los directivos de la entidad deberán procurar el cumplimiento por parte de todos los miembros de la entidad de los lineamientos y normas de seguridad de la información.

15.4. Toma de conciencia, educación y formación en la seguridad de la Información

Todos los empleados de la Lotería de Medellín y contratistas recibirán una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos en SI. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, en especial los asociados al manejo de contraseña segura, el cuidado ante archivos adjuntos maliciosos, el uso de mecanismos de doble autenticación, entre otros que se consideren importantes.

15.5. Proceso disciplinario

Los servidores de la Lotería de Medellín que incumplan con la política se someterán al proceso disciplinario de acuerdo con la normatividad vigente.

Adicionalmente pueden incurrir en responsabilidad civil, penal y fiscal.

15.6. Terminación o cambio de responsabilidades de empleo

La Dirección de Talento Humano debe realizar el proceso de desvinculación o cambio de labores de los funcionarios, llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, de forma ordenada, controlada y segura. En este caso, debe solicitar a la Oficina de las TIC la modificación o inhabilitación de usuarios en los sistemas de información a los que tiene acceso.

15.7. Devolución de Activos

- En el momento de desvinculación, vacaciones y licencias, los servidores públicos deben realizar la entrega de su puesto de trabajo al jefe inmediato o a quien este delegue.
- En caso de desvinculación deben encontrarse a paz y salvo en cuanto a los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.
- La Dirección de Talento Humano, debe informar con previa anticipación a la Oficina de las TIC para que se reciban los recursos tecnológicos que se le asignaron al funcionario.
- Los funcionarios que se desvinculan de la Entidad tienen prohibido eliminar la información que se encuentre en los equipos de cómputo. La Oficina de las TIC realizará una copia de respaldo o backup con el fin de disponer de dicha información, en caso de ser requerida.

Adicionalmente, se debe garantizar:

- Disponibilidad de toda la información que esté bajo la responsabilidad o propiedad de dicho integrante.
- Respaldo de la información de la cuenta de correo administrada por dicho integrante y de su disco duro si es necesario.
- Entrega de contraseñas si aplica.
- Borrado seguro de información garantizando que ninguna persona no autorizada pueda acceder a información crítica de la entidad.
- Transferencia de conocimiento cuando sea necesario.

16. Clasificación de información

La Lotería de Medellín debe generar y mantener actualizado un Registro de Activos de Información y un Índice de Información Clasificada y Reservada, estableciendo los niveles de criticidad dando cumplimiento a la normatividad legal (Ley 1712 de 2014) y al Modelo de Seguridad y Privacidad de la Información (MSPI).

La clasificación de la información permitirá asignar controles de seguridad proporcionales al nivel de sensibilidad, criticidad y riesgo que represente su divulgación, alteración o pérdida. La información se clasificará en las siguientes categorías:

- **Información Pública:** Información que, por mandato legal, normativo o decisión institucional debe ser de libre acceso para la ciudadanía. Su divulgación no genera riesgo alguno a la entidad.

- **Información de Uso Interno:** Información generada en el marco de las operaciones institucionales, destinada al uso de funcionarios, contratistas o terceros autorizados. Su divulgación no autorizada podría generar afectaciones leves en la operación de la entidad.

- **Información Reservada:** Información que se encuentra protegida por norma legal o contractual, cuyo acceso se limita únicamente a personal autorizado. Su divulgación no autorizada podría afectar de manera significativa la gestión institucional, la reputación o los derechos de los titulares de la información.

- **Información Clasificada o Confidencial:** Información de alto nivel de criticidad que, en caso de pérdida, alteración o divulgación no autorizada, puede generar impactos legales, financieros o reputacionales graves para la entidad. Incluye, entre otros, datos personales sensibles, información financiera crítica, claves de acceso, credenciales administrativas, como también a registros asociados al proceso de presorteo y sorteo, los cuales se consideran activos de máxima protección conforme a la NTC 6767:2024.

Controles asociados a la clasificación:

- **Etiquetado de Activos:** Toda la información física y digital deberá contar con un esquema de etiquetado o rotulado visible acorde a su nivel de sensibilidad.
- **Protección Técnica Reforzada:** La información Confidencial y Reservada exigirá controles técnicos obligatorios como Autenticación Multifactor (MFA) para su acceso, restricción de copias y cifrado criptográfico en tránsito y en reposo.
- **Enmascaramiento de Datos (Data Masking):** Para proteger la privacidad de los ganadores de la lotería y clientes en ambientes de pruebas, desarrollo o reportes públicos, se aplicarán técnicas de enmascaramiento o anonimización de datos personales.

17. Gestión de Activos

Los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, entre otros), estos activos se proporcionan para cumplir con los propósitos del Negocio.

Toda la información sensible de la Entidad, así como los activos donde se almacena y se procesa información, deben ser asignados a un responsable e inventariados y posteriormente clasificados.

17.1. Inventario de activos

La Lotería de Medellín debe contar con un documento donde se encuentren identificados los activos de información, el responsable, formato en el que se encuentra, y su clasificación.
Este documento, debe estar alineado con la normatividad sobre gestión documental, se debe revisar y si es del caso actualizar al menos 1 vez al año, o cuando se identifiquen necesidad de reflejar cambios en este. Igualmente se debe socializar a los terceros de interés previamente identificados y caracterizados.

17.2. Propiedad y Custodia de los Activos

- Los activos de información de la entidad deben tener un responsable asignado, el cual deberá procurar su buen uso, cuidado y preservación. En el caso de puestos de trabajo, el responsable será el usuario a quien se le asigne dicho equipo.
- La propiedad de los datos e información no estructurada (documentos ofimáticos) que radica en los discos duros de cada estación de trabajo corresponde igualmente al respectivo usuario.
- Las diferentes dependencias de la Lotería de Medellín deben actuar como propietarias de la información física y electrónica de la Entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- El inventario de los activos de información debe mantenerse actualizado, acogiendo las indicaciones para la clasificación de la información. Los recursos de procesamiento de información de la Entidad se encuentran sujetos a auditorías y a revisiones de cumplimiento por parte del personal asignado para esta labor.
- La Oficina de las TIC es la propietaria de los activos de información correspondientes a la infraestructura tecnológica (centro de datos, redes, etc.) y, en consecuencia, debe asegurar su apropiada operación y administración.
- La Oficina de las TIC es la autorizada para la instalación, configuración, cambio o eliminación de componentes de la plataforma tecnológica de la Lotería de Medellín.

- Los recursos tecnológicos de la Lotería de Medellín deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Entidad.
- La Oficina de las TIC debe recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando es solicitado formalmente. La custodia de los equipos está en cabeza del almacén.

17.3. Etiquetado o rotulado de Activos

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo con el Esquema de Clasificación adoptado por la Entidad. Estos procedimientos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las actividades de procesamiento de la información, almacenamiento y transmisión.

En el caso de activos tangibles, tales como equipos de cómputo, impresoras, dispositivos móviles, dispositivos extraíbles, etc. Se deberá realizar un etiquetado de tal manera que se identifique inequívocamente cada uno de estos. En el caso de que estos pertenezcan a algún proveedor, se deberá exigir esta actividad en el contrato respectivo y este debe ser realizado de acuerdo con las políticas de la Lotería de Medellín.

17.4. Devolución y Retiro de Activos

Todo recurso tecnológico entregado a funcionarios o terceros (portátiles, tokens, celulares) debe ser devuelto a la Oficina de las TIC o al Almacén al finalizar el vínculo laboral, contractual o al cambiar de rol. Está estrictamente prohibido que el usuario elimine información institucional de los equipos antes de entregarlos; la Oficina de las TIC será la encargada de realizar la copia de respaldo y el posterior borrado seguro del equipo.

18. Uso aceptable de los recursos tecnológicos

La Lotería de Medellín proporciona a los funcionarios, contratistas y terceros recursos tecnológicos de acuerdo con las funciones, responsabilidades y alcance de las actividades de cada uno realiza en la institución, con el único fin de llevar a cabo las labores de la Entidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

18.1. Reglas para el uso del Correo Electrónico

- Las cuentas de correo electrónico deben ser usadas para el desempeño de las funciones asignadas dentro de la Lotería de Medellín.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Lotería de Medellín y cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- El tamaño de los buzones de correo es determinado por la Oficina de las TIC de acuerdo con las necesidades de cada usuario y disponibilidad del servicio.
- El tamaño de los archivos adjuntos está sujeto a las características del servicio de correo electrónico contratado por la Lotería de Medellín.
- El envío de información corporativa debe hacerse exclusivamente desde la cuenta de correo que la Lotería de Medellín proporciona.
- El envío de mensajes institucionales internos y externos está a cargo del área correspondiente, y siempre deberán entregarse con la opción para que el usuario destinatario pueda darse de baja. Debe adoptarse la Política de Tratamiento de Datos Personales e Información, por parte del generador de los mensajes y usuarios de la información.
- La información que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por la Oficina de las TIC.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la Lotería de Medellín y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- La Entidad dispone de varias cuentas de correo para el envío de mensajes masivos, dicho envío será autorizado de acuerdo con las disposiciones de la entidad y se debe respetar el manual de imagen corporativa.

No está permitido

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad.

18.2. Uso de Internet

- La Lotería de Medellín podrá realizar monitoreo de los tiempos de navegación y páginas visitadas por parte de los funcionarios. Así mismo, podrá inspeccionar,

registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

- Los usuarios son responsables de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contraterceros, la legislación vigente y los lineamientos de seguridad de la información.
- Los usuarios de este servicio, no pueden asumir en nombre de la Lotería de Medellín, posiciones personales en encuestas de opinión, foros u otros medios similares.
-

No está permitido

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos, streaming, mensajería instantánea como Facebook, MSN Messenger, WhatsApp y otros similares, que no sean proporcionados por la entidad y que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio.
- La oficina de TIC´s habilitará páginas restringidas, previa solicitud escrita del director o responsable.
- El intercambio no autorizado de información de propiedad de la Lotería de Medellín, de sus clientes y/o de sus funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

18.3. Normas dirigidas a la Oficina de las TIC

- Eliminar de forma segura la información a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando ésta ya no sea vigente o cambia de usuario.
- Definir los métodos de cifrado de la información de la Entidad de acuerdo con el nivel de clasificación de los activos.

18.4. Normas dirigidas a la secretaria general

- Utilizar los medios apropiados para destruir o desechar correctamente la documentación física cuando se ha cumplido su ciclo de almacenamiento, con el fin de evitar la reconstrucción de esta, acogiéndose a procedimiento establecido para tal fin.
- Administrar el contrato de almacenamiento y resguardo de los documentos físicos del archivo histórico de la Entidad con el proveedor del servicio.

18.5. Normas dirigidas a todos los usuarios

- Acatar los lineamientos de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Entidad.
- La información física y digital de la Lotería de Medellín debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- Cuando se impriman, escaneen, saquen copias y envían faxes, se deben verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos, además recoger inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- En el momento en que los funcionarios se ausenten de sus puestos de trabajo, sus escritorios deben quedar libres de documentos y medios de almacenamiento utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

18.6. Normas para el manejo de los tokens de seguridad

- Los tokens deben ser entregados a los funcionarios designados para su uso, formalizando la entrega por medio de acta.
- Estos dispositivos son de uso exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.

- El almacenamiento de estos dispositivos debe efectuarse bajo estrictas medidas de seguridad, dentro de caja fuerte o escritorios con llave, de tal forma que se mantengan fuera del alcance de terceros no autorizados.
- Los Administradores de los tokens deben dar aviso a las entidades emisoras en caso de robo o pérdida, con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- Los Administradores de los tokens deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.
- Los usuarios deben devolver el token asignado en estado operativo al Administrador de los tokens cuando el vínculo laboral con Lotería de Medellín se dé por terminado o cuando haya cambio de cargo, para obtener el paz y salvo, el cual será requerido para legalizar la finalización del vínculo con la Entidad.
- Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado en el desarrollo de sus actividades como funcionarios de La Lotería de Medellín. En caso de que suceda algún evento irregular con los tokens, los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.
- Los usuarios no deben abrir los tokens, retirar la batería o placa de circuitos, ya que ocasionará su mal funcionamiento.

18.7. Manejo de medios magnéticos

Los medios magnéticos deben estar debidamente marcados y deben ser protegidos tanto al almacenarse como al transportarse.
De otra parte, se debe garantizar que el almacenamiento del hardware (si aplica) se realiza de acuerdo con las especificaciones de los fabricantes. (Política de respaldos).

18.8. Almacenamiento de la información

Toda la información propia de la gestión de la Lotería de Medellín debe residir en las bases de datos, en las carpetas de red asignadas a cada área, y/o en medios de almacenamiento externo entregado y/o respaldado por tecnología, nunca en los discos duros de las estaciones de trabajo, en cuyo caso se haría responsable al respectivo usuario en caso de presentarse pérdida o daño de información.

Las carpetas de red que se entregan a los funcionarios:

Carpeta temporal: Es para archivos temporales de uso institucional y será borrada el primer día hábil de cada mes.

Carpeta de red: Cada área tiene una carpeta asignada y en esta debe estar la información institucional que requiera ser respaldada.
Para archivos de información general se brinda el servicio de almacenamiento en la nube que podrá ser utilizado a discreción del usuario, está sujeta a la disponibilidad del proveedor del servicio.

18.9. Calidad del dato

Con el objetivo de mantener la transparencia y utilidad de las bases de datos de la entidad, los usuarios que ingresan y procesan información (especialmente en los procesos comerciales y de sorteos) deben garantizar la exactitud, consistencia e integridad de los datos ingresados a los sistemas.

19. Gestión De Medios Removibles (Dispositivos Extraíbles)

Evaluación: Requiere actualización para incluir controles tecnológicos (DLP/EDR) y cifrado obligatorio.

La Lotería de Medellín restringe el uso de medios de almacenamiento extraíbles (USB, discos duros externos, tarjetas SD) para mitigar el riesgo de fuga de información y la propagación de software malicioso.

19.1. Bloqueo por Defecto y Uso Autorizado

El uso de puertos USB para almacenamiento masivo estará bloqueado por defecto mediante herramientas de protección de endpoints (EDR/Antivirus corporativo). Su habilitación será estrictamente excepcional, temporal y requerirá la justificación del jefe de área y la aprobación de la Oficina de las TIC.

19.2. Cifrado Obligatorio

Todo medio extraíble autorizado que deba almacenar y transportar información "Uso Interno", "Reservada" o "Confidencial" fuera de las instalaciones de la entidad, deberá estar obligatoriamente cifrado (encriptado).

19.3. Disposición y Destrucción Segura

Si un medio extraíble institucional cumple su ciclo de vida o se daña, no podrá ser desechado directamente. Deberá entregarse a la Oficina de las TIC para su borrado seguro (criptográfico) o destrucción física certificada, imposibilitando la recuperación forense de los datos.

20. Control de acceso lógico y de red

La Lotería de Medellín adopta los principios de "Cero Confianza" (*Zero Trust*) y "Privilegios Mínimos". El control de acceso estará soportado por soluciones avanzadas de control de red (NAC) y gestión de accesos privilegiados (PAM) para garantizar la trazabilidad inmutable requerida en los procesos de sorteos y administrativos.

20.1. Control de Acceso a Redes y Evaluación de Postura

- Todo equipo de cómputo que intente conectarse a las redes de datos de la entidad (LAN, Wi-Fi o VPN) será evaluado en tiempo real por la solución de control de acceso a la red de la entidad.
- Para ser admitido, el dispositivo debe cumplir con las políticas de seguridad corporativas (*Endpoint Compliance*): estar en el dominio, contar con sistema operativo parcheado y antivirus/EDR activo y actualizado.
- Los dispositivos que no cumplan, o los equipos de terceros no autorizados, serán aislados o bloqueados automáticamente para prevenir accesos no autorizados.
- Está prohibido conectar dispositivos personales para labores no institucionales o intentar vulnerar los controles de red.

20.2. Registro, Suministro y Cancelación de Usuarios

- El ID de usuario (login) en todos los aplicativos y redes debe ser único, personal e intransferible.
- La creación, modificación o bloqueo de usuarios se hará bajo solicitud formal del jefe de área a través de la Mesa de Ayuda.
- **Bloqueo en Vacaciones y Retiros:** Las credenciales de acceso a la totalidad de los sistemas serán bloqueadas durante el tiempo de disfrute de vacaciones del empleado. En caso de retiro definitivo o cambio de funciones, los accesos serán inhabilitados en un lapso no superior a 24 horas tras la notificación de Talento Humano.

20.3. Gestión de Accesos Privilegiados y Administración Remota:

- Los derechos de acceso de "Superadministrador" están reservados exclusivamente para el personal técnico autorizado de la Oficina de las TIC.
- El uso de contraseñas de administrador compartidas, predeterminadas o almacenadas físicamente en "sobres cerrados" queda obsoleto y prohibido. Todas las credenciales críticas

(servidores, bases de datos de sorteos, *firewalls*) estarán custodiadas centralizadamente en la bóveda digital de la solución de administración de acceso privilegiado determinado por la entidad.

- Toda sesión administrativa crítica canalizada a través del PAM será grabada (video y *logs* de comandos), garantizando la auditoría inmutable de las acciones de los administradores.
- La administración remota solo se realizará mediante herramientas corporativas aprobadas. El uso de programas utilitarios privilegiados debe estar centralizado y controlado.

20.4. Carpetas de Red y Restricción a la Información:

- Cada dependencia cuenta con carpetas de red con permisos segmentados según las funciones del área. El acceso excepcional a terceros o a carpetas de otras áreas se otorgará solo bajo justificación del jefe de área (ej. accesos de solo lectura).
- Los aplicativos misionales deben contar con sistemas de menú y perfiles que restrinjan el acceso a las funciones (lectura, escritura, borrado) según el rol del usuario.

21.5. Autenticación, Gestión y Uso de Contraseñas:

- Todo acceso a sistemas de información, correo y VPN exigirá validación mediante **Autenticación Multifactor (MFA)**.
- La contraseña entregada por primera vez es temporal y el sistema obligará a su cambio en el primer inicio de sesión.
- Las contraseñas deben tener una longitud mínima de 10 caracteres, incluir combinaciones alfanuméricas y símbolos , y no hacer referencia a datos personales o secuencias predecibles.
- El sistema de gestión conservará un historial cifrado de contraseñas para prohibir la reutilización de claves anteriores.
-

20.6. Procedimiento de Ingreso Seguro a Aplicativos:

- Los mecanismos de ingreso a los sistemas informáticos no deben emitir mensajes de error que revelen información útil a un atacante (ej. indicar si falló el "usuario" o la "contraseña").
- Los sistemas deben contar con protección contra ataques de fuerza bruta (bloqueo por intentos fallidos) y registrar (log) tanto los ingresos exitosos como los denegados.

20.7. Revisión Periódica de Derechos de Acceso:

- La Oficina de las TIC, en conjunto con los líderes de proceso, realizará una revisión periódica de las matrices de roles y perfiles en todos los aplicativos. Esto asegura que los permisos sigan rigiéndose por el principio de privilegios mínimos a lo largo del tiempo.

21.8. Control de Acceso a Códigos Fuente:

- El código fuente de los aplicativos desarrollados por o para la entidad debe estar resguardado en repositorios centralizados con acceso estrictamente restringido.

- La entrega de librerías a desarrolladores debe hacerse mediante procedimientos seguros que protejan la propiedad intelectual y eviten modificaciones no autorizadas.

21. Criptografía y uso de controles criptográficos

El objetivo de la política sobre el uso de controles criptográficos es garantizar la confidencialidad, disponibilidad, integridad, autenticidad y el *no repudio* en el manejo de información de la Lotería de Medellín, de acuerdo con los niveles de clasificación y los medios utilizados para su almacenamiento, procesamiento y transmisión.

21.1. Alcance y Aplicación del Cifrado

- **Credenciales:** La entidad debe usar controles criptográficos de forma obligatoria para la protección de las credenciales de los usuarios en los sistemas informáticos.
- **Información No Pública:** Se velará porque la información clasificada o reservada sea cifrada, en lo posible, al momento de almacenarse y/o transmitirse por cualquier medio. Esto se aplicará siempre y cuando exista la respectiva viabilidad tecnológica y no se genere lentitud u otro tipo de dificultades en el desempeño de los sistemas.
- **Tipos de Datos:** La política aplica a toda la información de la entidad, tanto estructurada (bases de datos) como no estructurada (documentos electrónicos, escaneados, correo electrónico, entre otros).
- **Criterios de Selección:** Para determinar los mecanismos de cifrado, se tendrá en cuenta la normatividad colombiana sobre protección de datos personales, los estándares tecnológicos mundiales aplicables, el análisis de riesgos respectivo y la compatibilidad con la plataforma tecnológica.

21.2. Revisión de Algoritmos

El uso de algoritmos de cifrado (simétricos y/o asimétricos) y las longitudes de clave deberán ser revisadas periódicamente para aplicar las actualizaciones necesarias en atención a la seguridad requerida y a los avances en las técnicas de descifrado.

21.3. Gestión y Administración de Llaves Criptográficas

La Lotería de Medellín diseñará y construirá los procedimientos formales de control para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.

- **Solicitud:** La asignación de contraseñas de cifrado debe ser solicitada formalmente a la Mesa de Ayuda.
- **Responsabilidades de TIC:** Los responsables del sistema de cifrado establecerán los controles para asegurar el sistema, las contraseñas, y gestionar el acceso a funcionarios y terceros. Además, la Oficina de las TIC deberá registrar todas las actividades relacionadas con la administración y eliminación de llaves.

- **Responsabilidad del Usuario:** Las personas autorizadas deberán velar por la disponibilidad, integridad y confidencialidad de las contraseñas y de la información cifrada a su cargo.

21.4. Operación, Retención y Destrucción Segura

- La información cifrada o descifrada deberá ser tratada estrictamente de acuerdo con su nivel de clasificación y su eliminación deberá hacerse a través de un borrado seguro.
- **Deshabilitación:** Las llaves serán deshabilitadas y revocadas inmediatamente cuando se identifique algún riesgo de divulgación, o cuando se termine la relación laboral o contractual de la entidad con los empleados o terceros autorizados.

21.5. Reporte de Fallas y Riesgos

Los funcionarios, contratistas y terceros tendrán la responsabilidad ineludible de reportar, mediante los canales autorizados, las fallas reales o potenciales y los posibles riesgos del sistema de cifrado.

22. Seguridad física y del entorno

Las áreas destinadas al procesamiento, almacenamiento de información sensible y la infraestructura tecnológica de la Lotería de Medellín se consideran áreas de acceso restringido. Deben estar protegidas físicamente contra accesos no autorizados, daños e interferencias ambientales.

22.1. Perímetros y Controles de Acceso Físico

- El acceso a las instalaciones, en especial al centro de cómputo y cuartos de telecomunicaciones, exige autorización previa de la Oficina de las TIC. Los visitantes y proveedores deben registrar su ingreso y salida, y estar siempre acompañados por personal autorizado.
- La Subgerencia Financiera es responsable de velar por la efectividad de los controles de acceso físico en la entidad, incluyendo los accesos en horas no hábiles.
- Los funcionarios deben portar su carné de identificación en un lugar visible en todo momento y reportar inmediatamente su pérdida.
- En áreas de alta criticidad (ej. Centros de Datos), se reforzarán los controles de ingreso mediante autenticación de doble factor física (ej. biometría y tarjeta).

22.2. Seguridad de Oficinas, Recintos y Monitoreo Físico

- Se protegerá con cerraduras, control de acceso y sistemas de video-vigilancia (CCTV) el acceso a oficinas críticas como la Gerencia, Tesorería, cuartos de telecomunicaciones y, de manera primordial, los recintos destinados a los procesos de **presorteo y sorteo**.

- En caso de que los centros de datos operen mediante terceros (proveedores *Cloud/Colocation*), se les exigirá certificaciones internacionales que garanticen controles físicos estrictos, alarmas y protección ambiental.

22.3. Protección Ambiental y Suministro Eléctrico

- La infraestructura tecnológica y las áreas seguras deben estar protegidas frente a amenazas ambientales (incendios, inundaciones) mediante extintores, alarmas y la ejecución de un plan de mitigación basado en la matriz de riesgos.
- **Servicio Eléctrico:** La infraestructura eléctrica de las sedes (especialmente en el Valle de Aburrá) debe cumplir con la certificación RETIE. Los equipos de cómputo deben conectarse únicamente a las salidas respaldadas por la UPS institucional (tomas naranjados) para evitar daños por picos de voltaje y garantizar la continuidad. Queda prohibido conectar otros electrodomésticos en estas tomas.

22.4. Seguridad de Equipos y Cableado

- **Ubicación y Mantenimiento:** Los equipos deben situarse de forma que se minimicen los riesgos de daños físicos. El mantenimiento de redes, equipos y cableado (que debe estar protegido por canaletas y debidamente marcado) será realizado exclusivamente por personal idóneo autorizado por la Oficina de las TIC.
- **Movimiento de Activos:** La entrada, salida o reasignación de estaciones de trabajo y servidores requiere autorización documentada del Jefe de Área. La Oficina de las TIC es la única autorizada para realizar estos movimientos físicos y la custodia formal estará a cargo del Almacén.
- Está prohibido fumar, beber o consumir alimentos cerca de los equipos de la infraestructura tecnológica y estaciones de trabajo.

22.5. Seguridad de Equipos Fuera de las Instalaciones

- Los equipos corporativos retirados de las sedes (ej. portátiles para teletrabajo) deben contar con medidas preventivas obligatorias, como el cifrado de disco duro y contraseñas robustas. Dependiendo de la criticidad, la entidad considerará pólizas de aseguramiento contra robo o daño.

22.6. Política de Escritorio y Pantalla Limpia

- **Escritorio Limpio:** Los miembros de la entidad deben mantener su puesto de trabajo libre de documentos físicos confidenciales. Al retirarse de su puesto o finalizar la jornada, la información debe resguardarse en cajones bajo llave.
- **Pantalla Limpia:** Toda estación de trabajo deberá tener activado el protector de pantalla corporativo, el cual se bloqueará automáticamente tras un máximo de **tres (3) minutos** de inactividad, exigiendo contraseña para su desbloqueo. Adicionalmente, el usuario debe bloquear el equipo manualmente (Windows + L) al ausentarse y apagarlo al finalizar la jornada.

23. Seguridad de las operaciones

La Oficina de las TIC es la encargada de garantizar la operación segura, eficiente y resiliente de los recursos tecnológicos que apoyan los procesos misionales de la Lotería de Medellín, previniendo fallos y asegurando la continuidad del negocio.

23.1. Procedimientos Operativos Documentados

La operación y administración de la plataforma tecnológica debe estar respaldada por procedimientos documentados, actualizados y al alcance del personal autorizado. Estos deben incluir la instalación de software, gestión de copias de respaldo, ejecución de rutinas programadas, capacidades de procesamiento,reinicio/recuperación en caso de fallas y la ruta de escalamiento para situaciones excepcionales.

23.2. Protección contra Códigos Maliciosos y Ransomware

- **Defensa Activa:** Todos los recursos informáticos estarán protegidos por soluciones avanzadas de seguridad en el *endpoint* (EDR / Antivirus de nueva generación) debidamente licenciadas y actualizadas.
- **Monitoreo:** La entidad mantendrá un monitoreo continuo de la red y las aplicaciones (mediante IPS y WAF configurados con listas blancas/negras) para detectar y bloquear comportamientos anómalos o intentos de exfiltración de datos.
- Los usuarios tienen expresamente prohibido desactivar los controles de seguridad, introducir *software* malintencionado o abrir archivos adjuntos de dudosa procedencia. Cualquier sospecha de infección debe ser reportada de inmediato a la Mesa de Ayuda.

23.3. Respaldo de la Información y Ciberresiliencia

- La Lotería de Medellín ejecutará copias de respaldo (*backups*) periódicas de su información, software y configuraciones críticas, alineadas con la Política de Respaldos.
- **Inmutabilidad:** Para garantizar la recuperación ante ataques de *Ransomware*, los respaldos de los aplicativos críticos y bases de datos transaccionales (especialmente las asociadas a los sorteos) deben contar con características de **inmutabilidad** (no pueden ser cifrados, alterados ni borrados por atacantes) y cumplir, en lo posible, con la regla 3-2-1 (3 copias, en 2 medios distintos, 1 de ellos fuera de sitio o en la nube aislada).

23.4. Registro de Eventos (Logging) y Sincronización

- **Logs de Auditoría:** Los aplicativos críticos generarán registros (logs) inalterables que incluyan: usuario, fecha, hora, dirección IP, actividades realizadas e intentos fallidos de inicio de sesión. Esta información será centralizada y analizada mediante herramientas de correlación de eventos (SIEM).
- **Sincronización:** Todos los servidores, *firewalls* y sistemas de la entidad estarán sincronizados obligatoriamente con la hora legal de Colombia a través de servidores NTP confiables, garantizando la exactitud forense en caso de investigación.

23.5. Gestión de Vulnerabilidades Técnicas y Parcheo

- Se realizarán análisis periódicos de vulnerabilidades y pruebas de penetración (*Ethical Hacking*), ejecutadas preferiblemente por terceros independientes para garantizar imparcialidad.
- La Oficina de las TIC gestionará el ciclo de parcheo y actualización de los sistemas operativos y aplicaciones, priorizando la remediación de vulnerabilidades críticas basándose en el riesgo y la inteligencia de amenazas.

23.6. Separación de Ambientes y Control de Software

- Los ambientes de Desarrollo, Pruebas y Producción estarán estrictamente separados a nivel lógico y de red.
- **Protección de Datos Reales:** Queda prohibido el uso de datos reales y sensibles (ej. bases de datos de clientes) en los ambientes de desarrollo y pruebas. De ser estrictamente necesario, los datos deberán ser enmascarados o anonimizados previamente.
- La instalación y actualización de software en los sistemas operativos será exclusiva de la Oficina de las TIC, conservando siempre una estrategia de reversión (*rollback*) y el histórico de versiones anteriores.

23.7. Auditorías de Sistemas de Información

Las auditorías técnicas no deben interrumpir la operación del negocio. Todo plan de auditoría o escaneo de vulnerabilidades sobre el ambiente de producción debe ser aprobado por la Oficina de las TIC, ejecutándose preferiblemente en horarios de bajo impacto y con niveles de acceso estrictamente controlados.

24. Seguridad De Las Comunicaciones Y Transferencia De Información

La Oficina de las TIC establecerá los mecanismos para proveer la disponibilidad, integridad y confidencialidad de la información que se transporta a través de las redes de datos de la Lotería de Medellín, así como en su intercambio con terceros.

24.1. Seguridad y Segmentación de Redes

- **Microsegmentación:** Las plataformas tecnológicas estarán separadas en segmentos de red físicos y lógicos (ej. VLANs), independizando las redes de usuarios, servidores de producción, conexiones con terceros y redes inalámbricas.
- **Gestión Centralizada:** La red será administrada exclusivamente por la Oficina de las TIC o terceros bajo su estricta supervisión. Se deben monitorear los puertos lógicos y físicos para prevenir accesos no autorizados.
- **Monitoreo de Capacidad:** Se monitorearán continuamente los tiempos de respuesta, la capacidad y la latencia para garantizar una transmisión de datos constante y detectar posibles ataques de denegación de servicio (DDoS).

24.2. Seguridad de los Servicios de Red

- La gestión de servicios esenciales (DNS, DHCP, FTP, Impresión) se configurará bajo el principio de mínimos privilegios.
- **Servicio de Impresión:** Su uso es estrictamente institucional. Se restringe la impresión de correos electrónicos a casos indispensables, requiriendo revisión previa para evitar la fuga física de datos.

24.3. Intercambio y Transferencia de Información

- **Acuerdos con Terceros:** Todo intercambio de información electrónica con terceros (proveedores, entes de control) requerirá un acuerdo formal que establezca: estándares técnicos de transmisión, responsabilidades ante incidentes, mecanismos para garantizar la trazabilidad (evitar el *no repudio*) y el uso de encriptación cuando se transfiera información sensible.

24.4. Administración de Mensajería Electrónica Corporativa

El servicio de correo y colaboración en la nube es el canal formal de comunicación. Su administración técnica se regirá por las siguientes reglas:

- **Privilegios de Plataforma:** El rol de *Superadministrador* de la consola en la nube se asignará exclusivamente a quien determine la Jefatura de TIC, y este será quien otorgue los permisos de administración delegada.
- **Gestión de Grupos:** Se realizará un barrido periódico para eliminar grupos de correo vacíos, evitando confusiones en la entrega de mensajes. En los grupos masivos de comunicación institucional, los permisos de envío estarán restringidos únicamente a los propietarios del grupo.
- **Ciclo de Vida de Cuentas:** Se evitará el renombramiento de cuentas de correo; la mejor práctica será la eliminación y redireccionamiento. Antes de eliminar una cuenta, se verificará si posee archivos compartidos institucionales para transferir su propiedad y evitar pérdida de información.
- **Firmas y Confidencialidad:** Toda cuenta corporativa deberá incluir la firma estandarizada por la Oficina de Comunicaciones y un aviso legal de confidencialidad en el pie del mensaje.

25. Adquisición, Desarrollo Y Mantenimiento Seguro De Sistemas

La adquisición, desarrollo y mantenimiento de los sistemas de información de la Lotería de Medellín se regirá por el principio de "Seguridad desde el Diseño y por Defecto", garantizando que los controles de ciberseguridad se integren en todas las fases del ciclo de vida del *software* (SDLC).

25.1. Requisitos de Seguridad y Arquitectura

- Toda adquisición, desarrollo o contratación de aplicativos estará liderada y gestionada por la Oficina de las TIC.
- Desde la fase de concepción del proyecto, se deben identificar y documentar los requerimientos de seguridad, privacidad y trazabilidad, asegurando la compatibilidad con la arquitectura tecnológica y el licenciamiento legal de la entidad.

25.2. Ciclo de Desarrollo Seguro y Código Fuente

- Se adoptarán marcos de trabajo de desarrollo seguro para prevenir vulnerabilidades desde la escritura del código.
- Todo el código fuente (propio o contratado) debe administrarse mediante sistemas de control de versiones centralizados, aplicando restricciones de acceso por roles y manteniendo un historial inmutable de cambios.

25.3. Desarrollo Contratado Externamente

- Los proveedores externos de *software* deberán utilizar las metodologías, *frameworks* y estándares de seguridad definidos por la Oficina de las TIC.
- Los contratos incluirán cláusulas estrictas que garanticen la propiedad intelectual de la Lotería de Medellín sobre el código fuente, los entregables y la confidencialidad de la información.
- El personal de desarrollo externo tendrá acceso única y exclusivamente a los ambientes de desarrollo y pruebas, quedando estrictamente prohibido su acceso al ambiente de producción.

25.4. Protección de Transacciones y Servicios

- La información involucrada en las transacciones de servicios en línea y portales web debe protegerse contra enrutamientos errados, alteraciones fraudulentas y divulgación.
- Se garantizará el uso de certificados digitales emitidos por una Autoridad Certificadora confiable y protocolos de cifrado robustos de extremo a extremo para mantener la privacidad y el *no repudio* de las partes.

27.5. Pruebas de Seguridad y Aceptación

- Previo a su paso a producción, todo aplicativo nuevo o actualización mayor debe someterse a pruebas funcionales de seguridad (validación de login único, gestión de sesiones, roles de usuario) y pruebas de penetración (*Test de Penetración*) acordes a su criticidad.
- El paso a producción requiere obligatoriamente un acta de Prueba de Aceptación de Usuario (UAT) firmada por el líder del proceso misional.

25.6. Protección de Datos de Prueba

- Queda prohibido el uso de datos reales de producción (bases de datos con información personal o transaccional de sorteos) en los ambientes de desarrollo o pruebas.
- De ser estrictamente necesario utilizar una base de datos real para pruebas de estrés o errores, se deberá solicitar autorización a la Oficina de las TIC, aplicar técnicas de **enmascaramiento o anonimización** a los datos sensibles, y ejecutar un borrado seguro de dicha información inmediatamente al finalizar la sesión de pruebas.

26. Seguridad En La Relación Con Proveedores Y Terceros

La Lotería de Medellín establecerá mecanismos de control rigurosos en sus relaciones con proveedores, contratistas y terceros, asegurando que el acceso, procesamiento y almacenamiento de la información institucional se realice bajo estándares de seguridad iguales o superiores a los de la entidad.

26.1. Acuerdos de Confidencialidad y Cláusulas de Seguridad

Para cada uno de los contratos o convenios que la entidad firme, será obligatorio incluir cláusulas de confidencialidad (NDA). Además, se exigirá contractualmente el cumplimiento de la presente Política de Seguridad, acuerdos de nivel de servicio (SLA) en ciberseguridad y el respeto irrestricto a la Ley 1581 de 2012 (Protección de Datos Personales).

26.2. Responsabilidad de Supervisión

El supervisor designado para cada contrato debe hacerse responsable directo de verificar el cumplimiento de los lineamientos de Seguridad de la Información por parte del proveedor durante toda la ejecución del servicio. Esto incluye la validación de que el personal del tercero cuenta únicamente con los accesos estrictamente necesarios.

26.3. Seguridad en la Cadena de Suministro y Servicios en la Nube

Todo proveedor que ofrezca servicios en la nube (*Cloud Computing*) o alojamiento de infraestructura (Centros de Datos) para la Lotería de Medellín, deberá acreditar certificaciones de seguridad reconocidas internacionalmente (ej. ISO 27001, SOC 2, certificaciones Tier).

- La entidad se reserva el "Derecho a Auditar" los controles de seguridad tecnológica de sus proveedores críticos, previa notificación formal.

26.4. Gestión de Incidentes de Terceros y Fin del Contrato

- **Notificación de Brechas:** El proveedor tiene la obligación contractual de notificar a la Mesa de Ayuda de TI de la Lotería de Medellín, de forma inmediata, cualquier incidente de ciberseguridad que sufra en su propia infraestructura y que pueda comprometer los datos de la entidad.

- **Retorno y Borrado:** Al finalizar el contrato, el proveedor deberá devolver toda la información de propiedad de la Lotería de Medellín y emitir un certificado de borrado seguro, garantizando que no conserva copias no autorizadas.

27. Continuidad Del Negocio Y Gestión De Incidentes

- **Articulación de Procedimientos:** Los lineamientos tácticos y operativos para la notificación, escalamiento y contención de eventos de seguridad de la información se gestionarán de acuerdo con el **Procedimiento de Gestión de Incidentes de seguridad** vigente.
- **Ciberresiliencia:** Los aspectos para garantizar la disponibilidad operativa de la Lotería de Medellín frente a desastres o ciberataques críticos se gestionarán a través del **Plan de Continuidad del Negocio (BCP)** y el **Plan de Recuperación ante Desastres (DRP)**.

28. Cumplimiento Legal, Normativo Y Auditoría

La Lotería de Medellín velará por la estricta identificación, documentación y cumplimiento de toda la legislación aplicable en materia de seguridad, ciberseguridad y privacidad.

28.1. Derechos de Propiedad Intelectual y Licenciamiento

- Todos los derechos de propiedad intelectual de los productos y aplicaciones desarrolladas por empleados o subcontratistas son de propiedad exclusiva de la Lotería de Medellín.
- La Oficina de las TIC certificará que todo el *software* ejecutado en la entidad cuente con la respectiva licencia de uso o sea *software* libre autorizado. Queda estrictamente prohibida la instalación, copia o reproducción de *software* pirata o no autorizado en beneficio propio o de terceros.

28.2. Protección y Privacidad de Datos Personales (Habeas Data

- En cumplimiento estricto de la Ley 1581 de 2012 y sus decretos reglamentarios, la Lotería de Medellín aplicará todos los controles técnicos y organizativos necesarios para proteger los datos personales de sus clientes, apostadores, proveedores y colaboradores, garantizando su privacidad desde el diseño.

28.3. Protección de Registros y Gestión Documental

- La entidad dispondrá de un plan de gestión documental alineado a las Tablas de Retención Documental (TRD), asegurando la inmutabilidad, tiempos de retención y la recuperación segura de los registros críticos (incluyendo *logs* de auditoría y evidencias de sorteos).

28.4. Revisión Independiente (Auditoría Interna)

- La Oficina de Control Interno incluirá en sus planes anuales de trabajo metodologías y procedimientos para auditar los avances en ciberseguridad, evaluando de forma objetiva e independiente el cumplimiento de la presente política y la implementación del MSPI.

29. Referencias Normativas Y Responsables De La Política

29.1. Marco de Referencia

Esta política se soporta y actualiza basándose en los siguientes estándares:

- Norma ISO/IEC 27001:2022 (Controles de Seguridad de la Información y Ciberseguridad).
- Norma Técnica Colombiana NTC 6767:2024 (Procesos de juegos de suerte y azar).
- Modelo de Seguridad y Privacidad de la Información (MSPI) - MinTIC.
- Guías de la Superintendencia de Industria y Comercio (SIC) sobre gestión de incidentes.

29.2. Responsables del Documento

- **Generación y Actualización:** Oficina de las TIC / Oficial de Seguridad de la Información (CISO).
- **Socialización y Verificación:** Oficina de las TIC / Líderes de Proceso.
- **Aprobación Formal:** Gerente de la Lotería de Medellín / Comité Institucional de Gestión y Desempeño.