Region Metropolitana

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Fecha de aprobación: Diligencie la fecha de la aprobación - 29 del ENERO del 2026

1. INTRODUCCCIÓN

En la era digital actual, la seguridad de la información se ha convertido en una prioridad fundamental para las organizaciones, especialmente para aquellas que gestionan grandes volúmenes de datos y dependen de sistemas tecnológicos avanzados para sus operaciones. La Región Metropolitana Bogotá-Cundinamarca, es una entidad de orden público, creada a través del Acto Legislativo 02 del 22 de julio de 2020 y reglamentada por la Ley 2199 del 2022, cuya política pública aplicada, modificó el artículo 325 de la Constitución Política, creando la Región Metro*politana Bogotá-Cundinamarca.*

Bajo este contexto, este documento presenta el Plan Estratégico de Seguridad de la Información de la Región Metropolitana Bogotá - Cundinamarca, el cual abarca todos los sistemas, redes y datos relacionados con los hechos metropolitanos, se aplicará a todos los clientes internos y externos de la entidad.

Se enfocará en proteger los activos de información de la RMBC asegurando la confidencialidad, integridad y disponibilidad de la información, cumpliendo con la normatividad aplicable. Dado esto, el plan que suministra este documento se enfoca con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), incluyendo la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y el cumplimiento de las normativas legales y regulatorias aplicables, como la Ley 1581 de 2012 y el Decreto 1377 de 2013. Además, se considerarán las tendencias globales de ciberseguridad, como: aprendizaje automático de la seguridad, seguridad en IoT, expansión trabajo remoto, auge de la computación cuántica, evolución del phishing, enfoque en seguridad móvil, seguridad zero trust, carencia de habilidades y educación en ciberseguridad, y blockchain y la ciberseguridad.) y las mejores prácticas de estándares internacionales (IS0 27001, ISO 27002, NIST, COBIT, entre otros) para enfrentar los desafíos emergentes y proteger los activos de información de la Región Metropolitana, detalla las estrategias, procesos y recursos necesarios para la implementación del PESI (Plan Estratégico de Seguridad de la Información, asignando roles y responsabilidades claras a las áreas, equipos y personas clave dentro de la entidad. También se incluyen programas de capacitación y concienciación para promover una cultura de seguridad de la información entre todos los empleados y contratistas. La implementación de este plan es esencial para asegurar la protección de los activos de información y garantizar la resiliencia organizacional frente a riesgos cibernéticos y amenazas internas y externas.

2. METODOLOGIA UTILIZADA

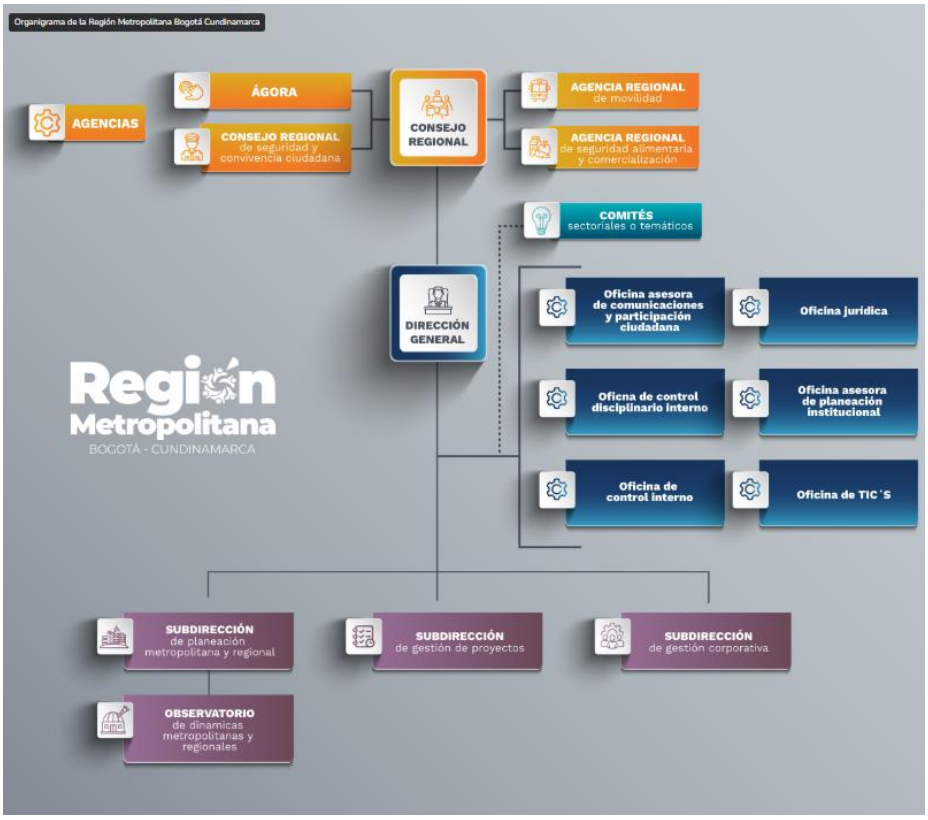
Para la construcción del Plan Estratégico de Seguridad de la Información (PESI) se desarrolló bajo una metodología que integra los principios y prácticas del marco ágil SCRUM, permitiendo un trabajo iterativo, colaborativo y orientado a la entrega de valor en la construcción del plan. Este enfoque se complementó con la aplicación de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), garantizando así que el PESI responda tanto a las necesidades estratégicas de la entidad como a los estándares y directrices nacionales en materia de seguridad de la información.

3. CONTEXTO ORGANIZACIONAL

El Plan Estratégico de Seguridad de la Información (PESI) se enmarca en la Ley 2199 de 2022, que establece el régimen especial para la Región Metropolitana Bogotá - Cundinamarca y define competencias en áreas como movilidad, servicios públicos, seguridad alimentaria, desarrollo económico, medio ambiente, seguridad ciudadana y ordenamiento territorial; todas ellas susceptibles de fortalecerse mediante el uso estratégico y seguro de las Tecnologías de la

Información y las Comunicaciones (TIC). En este contexto, nuestro mapa de procesos permite impulsar el cumplimiento de su misión, visión y funciones mientras se consolida un ejercicio integral de estructuración del Sistema Integrado de Planeación y Gestión. Paralelamente, se trabaja en la definición de los procesos y procedimientos detallados por área, asegurando que el PESI se articule de manera efectiva con el modelo de gestión de calidad y con las directrices nacionales en materia de seguridad de la información.

1. Estructura Organizacional[1]



La Región Metropolitana Bogotá - Cundinamarca está constituida por el Consejo Regional conformado por las siguientes agencias:

- ÁGORA
- Consejo Regional de Seguridad y Convivencia Ciudadana
- Agencia Regional de Movilidad
- Agencia Regional de Seguridad Alimentaria y Comercialización

La Dirección General de la Región Metropolitana Bogotá – Cundinamarca quien lidera las siguientes Oficinas y Subdirecciones:

- Oficina Asesora de Comunicaciones y Participación Ciudadana
- Oficina Jurídica
- Oficina de Control Disciplinario Interno
- Oficina Asesora de Planeación Institucional
- Oficina de Control Interno

[1] Fuente: https://regionmetropolitana.gov.co/entidad/organigrama, enero 2026

- Oficina de Tecnologías de la Información y Comunicaciones
- Subdirección de Planeación Metropolitana y Regional
- Subdirección de Gestión de Proyectos
- Subdirección de Gestión Corporativa
- Observatorio de Dinámicas Metropolitanas y Regionales

4. OBJETIVO

Establecer la estrategia, lineamientos y acciones necesarias para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad, mediante la planeación de la seguridad de la información (PESI) de la Región Metropolitana Bogotá – Cundinamarca, en cumplimiento de la normativa vigente y en concordancia con los requisitos de la norma ISO 27001:2022, fortaleciendo así la gestión de riesgos, la protección de los activos de información y la confianza de los grupos de interés.

5. OBJETIVOS ESPECÍFICOS

- **Alinear, dirigir y supervisar la elaboración, implementación y mejora continua de la estrategia y políticas de seguridad de la información**: estas actividades se desarrollarán en concordancia con las directrices, objetivos y acciones definidas en el PETI de la RMBC garantizando la protección de los activos de información y el cumplimiento normativo.
- **Desarrollar e implementar estrategias de control de acceso y autenticación**: Asegurar que solo los usuarios autorizados tengan acceso a la información y sistemas mediante la adopción de métodos de autenticación multifactorial (MFA).
- **Realizar evaluaciones periódicas y gestionar vulnerabilidades**: Evaluar regularmente la efectividad de las medidas de seguridad implementadas mediante evaluaciones y pruebas de penetración, y establecer un proceso para la gestión de riesgos y la mitigación de vulnerabilidades.
- **Promover una cultura de seguridad de la información**: Desarrollar programas de capacitación continua y campañas de concientización para todos los colaboradores, asegurando que comprendan la importancia de proteger los activos de información y se sientan responsables de reportar cualquier incidente o vulnerabilidad.

6. ALCANCE

El alcance del Plan Estratégico de Seguridad Informática de la Región Metropolitana Bogotá-Cundinamarca abarca todos los sistemas, redes y datos relacionados con la entidad, se enfocará en proteger los activos de información, como sistemas de información, equipos de almacenamiento, networking, seguridad perimetral y de datos, asegurando la confidencialidad, integridad y disponibilidad de la información.

Para la ejecución de este plan se debe involucrar a todas las áreas de la entidad y a los terceros que tengan acceso a la información y los datos de la Región Metropolitana, para implementar medidas tendientes a garantizar la seguridad y privacidad de la información mediante evaluaciones periódicas y procesos de mejora continua.

7. DEFINICIONES[2]

[2] Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información, MINTIC. https://gobiernodigital.mintic.gov.co/692/articles-401770_recurso_1.pdf

- **Activo de información:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **Modelo de Seguridad y Privacidad de la Información**: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

SIGLAS

- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **SGSI:** Sistema de gestión de seguridad de la información

8. MARCO NORMATIVO Y LEGAL

Protección de datos

- Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- 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.

Seguridad informática

- CONPES 3995 de 2019. Política nacional de confianza y seguridad digital.
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Circular 01 de 2022 - Departamento Administrativo de la Presidencia de la República. Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.

Sistema de gestión de seguridad de la información

- Directiva 02 de 2022 - Presidencia de la República. Reiteración de la política pública en materia de seguridad digital.
- Decreto 338 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el Título 21 a la Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Resolución 746 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamentos adicionales a los establecidos en la Resolución No. 500 de 2021.
- Decreto 767 de 2022 - Presidencia de la República. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 02277 de 2025. “Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”

9. CONTEXTO DE LA ENTIDAD

La entidad inició su operación a finales del año 2023, en el marco de un proceso de modernización institucional que incluye la adopción de políticas y prácticas alineadas con estándares internacionales en materia de seguridad y privacidad de la información.

Actualmente, se encuentra en fase de construcción e implementación de su Modelo de Seguridad y Privacidad de la Información (MSPI), proceso que se desarrolla de manera articulada con la normatividad vigente.

La publicación de la Resolución 02277 de 2025, que actualiza el Anexo 1 de la Resolución 500 de 2021 y deroga disposiciones previas relacionadas con el MSPI, ha marcado un hito en el proceso institucional. Esta actualización implica el tránsito de un modelo basado en la norma ISO 27001:2013 a uno fundamentado en los lineamientos y requisitos de la ISO 27001:2022, estableciendo nuevos parámetros para la gestión de la seguridad de la información.

En este escenario, la entidad se enfrenta al reto de consolidar un modelo robusto que garantice la protección, integridad, disponibilidad y confidencialidad de la información, en concordancia con las exigencias regulatorias y las mejores prácticas internacionales.

10. ANÁLISIS DE LA ENTIDAD

Situación Actual

La entidad se encuentra en una fase de desarrollo y consolidación de su Modelo de Seguridad y Privacidad de la Información (MSPI), en la cual se están definiendo, documentando e implementando los procesos, controles y políticas necesarios para garantizar la protección de los activos de información. Entre estos instrumentos estratégicos se incluye el Plan Estratégico de Seguridad de la Información (PESI), que busca establecer lineamientos claros para la gestión de riesgos, la respuesta a incidentes y la continuidad del negocio. Este proceso, al encontrarse en etapa temprana, requiere una planificación estructurada y la participación de todas las áreas de la entidad.

El contexto normativo actual, impulsado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establece la obligación de adoptar un enfoque más moderno y alineado con los requisitos de la norma ISO 27001:2022. Este cambio representa una oportunidad para implementar desde el inicio las mejores prácticas internacionales en gestión de seguridad de la información, evitando modelos desactualizados. Sin embargo, también implica un desafío significativo, ya que requiere ajustar la planeación, la asignación de recursos y la capacitación del personal para asegurar una transición eficiente y el cumplimiento estricto de las disposiciones vigentes.

Fortalezas	Oportunidades
• Voluntad institucional de alinearse con estándares internacionales.	• Actualización normativa que promueve el uso de estándares globalmente reconocidos.
• Oportunidad de diseñar el Modelo de Seguridad y Privacidad de la Información	• Integración de tecnologías y soluciones modernas de seguridad sin depender de sistemas antiguos.

Fortalezas	Oportunidades
desde cero incorporando los requisitos de la ISO 27001:2022.	
• Reciente creación de la entidad, lo que evita procesos heredados y obsoletos.	• Posicionamiento como entidad de referencia en seguridad y privacidad de la información en el sector público.
Debilidades	**Amenazas**
• Falta de madurez en los procesos de seguridad de la información debido a la corta trayectoria institucional.	• Brecha temporal entre la exigencia normativa y la capacidad de implementación efectiva.
• Limitada experiencia previa en la aplicación práctica de los controles ISO 27001:2022.	• Creciente sofisticación de las amenazas cibernéticas.
• Escasez de recursos humanos especializados en ciberseguridad y gestión de la información.	• Posible resistencia al cambio por parte del personal frente a nuevos procesos y controles.

MATRIZ DOFA – Plan Estratégico de Seguridad de la Información (PESI)
Fuente: Elaboración propia Oficina TIC – RMBC

11. ESTRATEGIA DE SEGURIDAD DIGITAL – REGIÓN METROPOLITANA BOGOTÁ – CUNDINAMARCA

Nuestra estrategia está enfocada en fortalecer la protección de la información institucional garantizando su confidencialidad, integridad y disponibilidad, mediante la adopción de prácticas seguras por parte de todas las partes interesadas internas y externas.

Líneas estratégicas:

Gobernanza y cumplimiento normativo

- Alinear las políticas y procedimientos de seguridad de la información con la Ley 2199 de 2022, los estatutos de la Entidad y las disposiciones del Consejo Regional de la RMBC.

- Mantener un monitoreo constante de cambios normativos y actualizaciones tecnológicas que puedan impactar la seguridad digital de la entidad.

Cultura y corresponsabilidad en seguridad de la información

- Implementar programas de sensibilización y capacitación periódica dirigidos a funcionarios, contratistas, proveedores y aliados.

- Promover buenas prácticas digitales como uso de contraseñas seguras, manejo responsable del correo electrónico y prevención de ciberataques.

Protección y gestión de activos de información

- Clasificar la información institucional y aplicar controles según su nivel de criticidad.

- Garantizar copias de seguridad, control de accesos y mecanismos de cifrado para información sensible.

Prevención y respuesta ante incidentes

- Definir un procedimiento de gestión de incidentes de seguridad digital, incluyendo detección, contención, análisis y recuperación.

- Establecer canales de reporte rápido para que cualquier parte interesada pueda alertar sobre amenazas o vulnerabilidades.

12. DEFINICIÓN DE LAS ACTIVIDADES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FINAL
1. Establecimiento del Comité de Seguridad **Descripción:** Conformar el comité de seguridad de la información, este comité será responsable de supervisar la implementación de la Política de Seguridad de la Información y coordinar las acciones necesarias para su aplicación.	**Responsable:** Alta Dirección Oficina de TIC	01-04-2026	30-12-2026
2. Segmentación de Redes **Descripción:** Segmentar físicamente la Red de Datos en dos; una encargada de la red cableada desde switches de distribución y de Core y otra en wifi. Para cada una de ellas, se aislarán las redes y se permitirá comunicación según políticas y vlans, de igual manera se segmentará la red según áreas que componen la institución, según ubicación física, permisos de acceso y servicios prestados ante el usuario final. Esto implica direccionamientos IP por segmentos y vlans de acceso, también se monitoreará configuraciones, accesos y tráfico de red que permita seguimiento, control y permisos a los usuarios según el segmento al que pertenezcan	**Responsable:** Oficina de TIC	01-10-2026	30-12-2026
3. Gestión de Vulnerabilidades **Descripción:** Realizar pruebas de penetración regulares para identificar y mitigar posibles vulnerabilidades en los sistemas y aplicaciones. Establecer un proceso para la gestión de parches, asegurando que todas las actualizaciones de seguridad se apliquen de manera oportuna.	**Responsable:** Oficina de TIC	01-04-2026	30-12-2026

ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FINAL
4. Capacitación y Concientización **Descripción:** Desarrollar y ejecutar una jornada de capacitación para todos los funcionarios y contratistas en prácticas de seguridad de la información. Organizar una campaña de concientización, además de comunicar de manera constante a los colaboradores de la RMBC sobre la importancia de la seguridad de la información.	**Responsable:** Oficina de TIC	01-04-2026	30-12-2026
5. Cumplimiento Normativo **Descripción:** Definir las cláusulas contractuales enfocadas en seguridad de la información y semestralmente validar su actualización.	**Responsable:** Oficina Jurídica	01-11-2026	30-12-2026

13. PARTES INTERESADAS

En el marco del Plan Estratégico de Seguridad de la Información (PESI) de la Región Metropolitana Bogotá – Cundinamarca, se reconocen como partes interesadas internas y externas a todas aquellas personas, grupos u organizaciones que, de manera directa o indirecta, participan o se ven impactadas por la gestión de la seguridad de la información. Entre ellas se encuentran los funcionarios, contratistas, proveedores, entes de control, entidades asociadas y la ciudadanía en general, quienes tienen un papel fundamental en garantizar la confidencialidad, integridad y disponibilidad de la información institucional. La identificación y consideración de estas partes interesadas se realiza en coherencia con la Ley 2199 de 2022, los estatutos de funcionamiento y la estructura organizacional aprobada por el Consejo Regional.

Así mismo, el PESI establece que todos los funcionarios, contratistas, proveedores y cualquier tipo de colaborador deberán adoptar e implementar de manera responsable los lineamientos, políticas y procedimientos relacionados con la seguridad de la información. Esta corresponsabilidad busca fomentar una cultura organizacional orientada a la protección de los activos de información, minimizando riesgos y asegurando el cumplimiento normativo. La interacción activa y el compromiso de cada parte interesada son esenciales para fortalecer la gestión de la seguridad y contribuir al logro de los objetivos estratégicos de la Entidad.

14. CONCLUSIONES

La entidad se encuentra en una etapa clave para consolidar el Plan Estratégico de Seguridad de la Información PESI, aprovechando la reciente creación de la entidad nos permite adoptar de forma directa y sin rezagos los lineamientos más actuales de la ISO 27001:2022. El marco normativo establecido por la Resolución 02277 de 2025 publicada por MinTic representa tanto un desafío como una oportunidad, pues exige un cambio en la estructura y enfoque de los controles de seguridad, alineándolos con estándares internacionales más robustos y actualizados.

El análisis DOFA evidencia que, aunque existen debilidades propias de una organización en formación, como la falta de madurez en los procesos y la escasez de personal especializado, también se cuenta con fortalezas significativas, como la flexibilidad para diseñar el modelo desde cero y la disposición institucional para cumplir con la normativa. Asimismo, las oportunidades derivadas de la actualización normativa y la incorporación de tecnologías modernas pueden ser factores decisivos para lograr una implementación exitosa.

15. REFERENCIAS

- A través de la Resolución 02277 de 2025, el Ministerio TIC actualiza el Modelo de Seguridad y Privacidad de la Información: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/403045:A-traves-de-la-Resolucion-02277-de-2025-el-Ministerio-TIC-actualiza-el-Modelo-de-Seguridad-y-Privacidad-de-la-Informacion

- Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información: https://www.mintic.gov.co/portal/715/articles-403045_recurso_1.pdf

- Guía para la construcción del Plan de Seguridad y Privacidad de la Información MinTic 2025: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

- Norma ISO/IEC 27001: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos: https://www.iso.org/isoiec-27001-information-security.html

- Ley 1581 de 2012: Ley de Protección de Datos Personales en Colombia: https://www.funcionpublica.gov.co/documents/418537/0/Ley+1581+de+2012.pdf

- Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%201377%20DEL%202013.pdf