RENOBO

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ

Integración de los Planes Institucionales y Estratégicos al Plan de Acción Institucional

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)

2026–2029

Dirección Administrativa y de TICs

Versión 1.0, enero de 2026

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Tabla de contenido

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

1. Resumen ejecutivo

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) 2026–2029** define las directrices para gestionar riesgos críticos que afectan la **confidencialidad, integridad, disponibilidad y privacidad** de la información institucional. El PTRSPI se fundamenta en **ISO/IEC 27001:2022**, **ISO/IEC 27002:2022**, el **Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC** y los lineamientos de la **Circular 007 de 2024**; con ello garantiza **trazabilidad normativa y contractual** y **defendibilidad** ante auditorías internas y externas.

El plan se **articula** con el **PETI 2026–2029** y el **PSPI**, soportando el objetivo estratégico **EO0203**: *"Fortalecer la capacidad de la infraestructura tecnológica, promoviendo la implementación de tecnologías de última generación"*. La gestión del riesgo se ejecuta sobre una **arquitectura moderna** que integra **nube híbrida**, **API Management** y **Centro de Datos Empresarial (CDE)**, habilitando **interoperabilidad** y **trazabilidad del dato**.

Como parte de la **transformación digital** institucional, el PTRSPI consolida **resiliencia tecnológica**, **seguridad digital** y **accesibilidad** (**WCAG 2.1 AA**), bajo **gobernanza** del **Mesa de trabajo SGSI** y del **Comité Institucional**, con evidencias en actas y **control de versiones** conforme al **control 5.3** de **ISO/IEC 27001:2022**.

En 2025 se desarrolló la fase inicial del Plan de Continuidad del Negocio (BCP) y se elaboró el primer borrador del DRP, el cual quedó en fase de formulación preliminar sin aprobación formal. En 2026, el DRP se consolida como documento normativo y operativo, alineado con ISO/IEC 27001:2022 y el Modelo MSPI.

Incorporar los riesgos críticos del PTRSPI al mapa de riesgos institucional durante la vigencia 2026, en cumplimiento de la metodología DAFP v7, la Circular 007/2024 y las cláusulas 6.1.3 y 5.3 de ISO/IEC 27001:2022, garantizando la mejora continua y la trazabilidad documental.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

1.1. Riesgos críticos priorizados

- **R-01:** Indisponibilidad de servicios críticos
- **R-02:** Compromiso de cuentas de correo institucional
- **R-03:** Vulnerabilidades críticas en portal web
- **R-04:** Configuración insegura en nube pública/privada
- **R-05:** Datos sin cifrado en tránsito o reposo.

1.2. Decisiones estratégicas

- **Mitigar** riesgos **altos y extremos** mediante controles **ISO/IEC 27001:2022**
- **Transferir** riesgos residuales mediante **contratos y pólizas**
- **Evitar** riesgos mediante **rediseño de procesos críticos**
- **Aceptar** únicamente riesgos **bajos** y dentro de lo aprobado por **Alta Dirección**.

1.3. Impacto esperado en KPIs

- **≥ 90%** de riesgos críticos mitigados
- **≥ 90%** de controles ISO implementados
- **Nivel de madurez MSPI** ≥ 4 (Optimizado)

El ***PTRSPI*** incorpora los resultados del **autodiagnóstico MSPI 2025**, las **brechas FURAG** y los hallazgos de auditorías internas, proyectando acciones para cerrar no conformidades y prevenir hallazgos recurrentes. El cronograma detallado de actividades, responsables y entregables se encuentra en el archivo **“Plan de Acción**

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

proceso gestión de TI 2026.xlsx”, repositorio oficial del SGSI, garantizando trazabilidad y defendibilidad ante entes de control.

1.4. Propósito

Definir y ejecutar el **tratamiento de riesgos altos y extremos** para garantizar la **continuidad del negocio**, la **protección de datos personales** y el **cumplimiento normativo**; articulando el PTRSPI con el **PSPI** y el **PETI** para sostener la **transformación digital** sobre infraestructura de **nube híbrida, API Management y CDE**, con gobernanza en comité o mesa de trabajo y evidencias auditables.

1.5. Alcance

- **Procesos incluidos:** Todos los procesos misionales, estratégicos y de apoyo.
- **Procesos excluidos:** Aplicaciones históricas sin datos activos y sistemas fuera de operación.
- **Activos críticos:** Infraestructura TI, ERP JSP7, SGDEA TAMPUS, correo institucional y nube híbrida (Google Workspace, SaaS críticos).
- **Horizonte temporal:** Vigencia 2026–2029, con revisión trimestral y actualización anual.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

2. Objetivos

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** tiene como propósito orientar la gestión integral de riesgos que afectan la seguridad y privacidad de la información institucional, asegurando **continuidad del negocio**, **protección de datos personales** y **cumplimiento normativo**. Para ello, se establecen los siguientes objetivos:

2.1. Objetivo general

Definir y ejecutar el tratamiento de riesgos altos y extremos, alineado con:

- **ISO/IEC 27001:2022** (Cláusulas 4–10 y 6.1.3/6.3)
- **ISO/IEC 27002:2022** (93 controles en 4 dominios)
- **Modelo de Seguridad y Privacidad de la Información (MSPI)** del MinTIC Garantizando trazabilidad con la **Declaración de Aplicabilidad (SOA)** y evidencias auditables.

2.2. Objetivos específicos

2.2.1. Identificar, valorar y clasificar riesgos de seguridad y privacidad en todos los procesos

Identificar, analizar, valorar y clasificar anualmente los riesgos de seguridad y privacidad en todos los procesos misionales, estratégicos y de apoyo, aplicando la Guía DAFP v7 (2027) y la metodología institucional, generando una matriz de riesgos consolidada y actualizada como insumo directo para la Declaración de Aplicabilidad (SOA) y el Plan de Tratamiento de Riesgos (PTR).

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

2.2.2. Orientar la implementación de controles *ISO / IEC 27002:2022*

Orientar la implementación y verificación de controles del Anexo A de ISO/IEC 27002:2022 en los activos críticos institucionales (infraestructura TI, ERP JSP7, SGDEA-TAMPUS, correo institucional y nube híbrida), asegurando la mitigación de riesgos altos y extremos y la documentación de evidencias técnicas en el SOA actualizado.

2.2.3. Fortalecer la cultura organizacional

Fortalecer la cultura organizacional en gestión de riesgos de seguridad y privacidad mediante programas de sensibilización y capacitación alineados con el ***MSPI*** y el ciclo ***PHVA (Planear–Hacer–Verificar–Actuar)***. Alcanzar una cobertura anual mínima del 80% de colaboradores y evidenciar mejoras en la comprensión y aplicación de los controles.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

3. Alineación estratégica – entendimiento estratégico

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** se articula con los instrumentos estratégicos y normativos que orientan la transformación digital y la resiliencia tecnológica de la **Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C**. Esta alineación asegura que la gestión de riesgos no sea un ejercicio aislado, sino un habilitador transversal para el cumplimiento de los objetivos institucionales y la generación de valor público.

3.1. Contribución estratégica

- **Pilar de Excelencia Operacional:** El PTRSPI fortalece la eficiencia operativa mediante la mitigación de riesgos críticos que afectan la disponibilidad, confidencialidad e integridad de la información.
- **Transformación digital:** El plan acompaña la modernización tecnológica definida en el **PETI 2026–2029**, priorizando interoperabilidad, trazabilidad del dato y seguridad digital sobre una arquitectura moderna basada en **nube híbrida**, **API Management** y **Centro de Datos Empresarial (CDE)**.
- **Objetivo EO0203:** Se soporta la meta de “Fortalecer la capacidad de la infraestructura tecnológica, promoviendo la implementación de tecnologías de última generación”, garantizando que la gestión de riesgos evolucione sobre plataformas robustas y escalables.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

3.2. Articulación normativa y distrital

- Se adoptan los lineamientos de la **Circular 007 de 2024** de la Consejería Distrital de TIC, que exige accesibilidad digital (WCAG 2.1 AA), interoperabilidad y seguridad de la información como condiciones obligatorias para los PETI distritales. Estas disposiciones se integran al ciclo **PHVA (Planear–Hacer–Verificar–Actuar)** y se evidencian mediante actas de comité o mesa de trabajo y control de versiones conforme al control 5.3 de **ISO/IEC 27001:2022**.

3.3. Sincronización con planes institucionales

- **PETI 2026–2029:** El PTRSPI contribuye al **OE-TI 3: Resiliencia y seguridad digital**, mediante la implementación de controles ISO/IEC 27001:2022 y la mitigación de riesgos críticos que afectan la continuidad del negocio.
- **PSPI 2026–2029:** Integra los lineamientos del **MSPI** y soporta los KPIs estratégicos definidos en el PSPI, tales como:
    - % riesgos críticos mitigados (Meta: ≥90%)
    - % controles ISO implementados (Meta: ≥90%)
    - Nivel de madurez MSPI (Meta: ≥4 – Optimizado).

Trazabilidad EO0203–PTRSPI. Las actividades del Capítulo 8 materializan el EO0203 al modernizar infraestructura sobre **nube híbrida**, **API Management** y **Centro de Datos Empresarial (CDE)**, asegurando **interoperabilidad** y **trazabilidad del dato** con gobernanza de la **Mesa de trabajo SGSI** (control 5.3) y metas de **continuidad, acceso, vulnerabilidades, nube y criptografía**.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

3.4. Metodología y defendibilidad

El PTRSPI se sincroniza con las fases metodológicas del MinTIC para los PETI (**Planear–Analizar–Construir–Socializar**), asegurando trazabilidad entre diagnóstico, brechas FURAG, cronograma de implementación y anexos técnicos. Esta integración permite demostrar cumplimiento normativo y contractual ante auditorías internas y externas, reforzando la gobernanza del SGSI.

La reincorporación del DRP en 2026 responde a la necesidad de completar la implementación que no se logró en 2025, donde solo se alcanzó la fase diagnóstica y formulación preliminar. El DRP ahora se integra como mecanismo operativo para riesgos altos y extremos, con cronograma de pruebas y evidencias auditables.

Actividad PTRSPI	OE-TI (PETI 2026-2029)	KPI PSPI
Actualización de herramienta/formato para inventario de activos	OE-TI 3: Resiliencia y seguridad digital	% activos clasificados ≥95%
Sensibilización y capacitación sobre gestión de riesgos	OE-TI 4: Excelencia operacional	Nivel de madurez MSPI ≥4
Actualización del inventario de activos por proceso	OE-TI 3: Resiliencia y seguridad digital	% activos clasificados ≥95%
Actualización de riesgos priorizados con Análisis de Impacto del Negocio (BIA)	OE-TI 3: Resiliencia y seguridad digital	% riesgos críticos mitigados ≥90%
Asignación de controles ISO en activos moderados a extremos	OE-TI 3: Resiliencia y seguridad digital	% controles ISO implementados ≥90%

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Actividad PTRSPI	OE-TI (PETI 2026-2029)	KPI PSPI
Verificación y actualización de la Política de Gestión de Riesgos	OE-TI 4: Excelencia operacional	Nivel de madurez MSPI ≥4
Articulación con Alta Consejería TIC para datos abiertos	OE-TI 2: Transformación de datos	KPI Transparencia y datos abiertos
Documentación de la guía para administración de riesgos y gestión de incidentes	OE-TI 4: Excelencia operacional	Nivel de madurez MSPI ≥4
Incorporación de riesgos críticos al mapa institucional (con BIA y DRP)	OE-TI 3: Resiliencia y seguridad digital	% riesgos críticos mitigados ≥90%

Tabla 1 - Alineación estratégica: PTRSPI ↔ PETI ↔ PSPI

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

4. Glosario

Además de las definiciones contenidas en la PL-08 Política para la Administración de Riesgos V 03 y en la guía que, para la administración de riesgos de seguridad y privacidad de la información, la cual será documentada en 2025, se incluyen las siguientes definiciones:

Concepto	Definición
Riesgo	Es toda posibilidad de ocurrencia de aquella situación que puede afectar el desarrollo normal de la entidad y el logro de sus objetivos.
Seguridad de la Información	Conjunto de técnicas y métodos encaminados a la prevención de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión.
MFA o Autenticación multifactor	Mecanismo que requiere dos o más factores independientes para validar identidad.
DRP	Plan de recuperación ante desastres

Tabla 2 – Glosario

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

5. Normatividad aplicable

El **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** se fundamenta en un marco normativo robusto que garantiza la protección de la información institucional, la continuidad del negocio y el cumplimiento contractual. Este marco integra:

5.1. Normas internacionales

- **ISO/IEC 27001:2022**: Cláusulas 4.3 (alcance), 5.3 (roles y responsabilidades), 6.1.3 (tratamiento de riesgos), 8.4 (continuidad) y 9.1 (monitoreo). Requisitos para SGSI: alcance, roles, tratamiento de riesgos, continuidad, auditoría.
- **ISO/IEC 27002:2022**: Controles aplicables, incluyendo 5.19 (relación con proveedores), 5.23 (seguridad en la nube), 5.30 (continuidad del negocio), 8.2 (control de acceso), 8.8 (gestión de vulnerabilidades) y 8.24 (criptografía). Controles aplicables: continuidad, nube, vulnerabilidades, cifrado, control de acceso, privacidad

5.2. Normas nacionales y distritales

Norma	Entidad que la expide / Ámbito	Descripción / Alcance
Ley 1273 de 2009	Congreso de la República (Nacional)	Tipifica los delitos informáticos y protege la información y los datos.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Norma	Entidad que la expide / Ámbito	Descripción / Alcance
Ley 1581 de 2012	Congreso de la República (Nacional)	Establece el régimen general de protección de datos personales.
Ley 1712 de 2014	Congreso de la República (Nacional)	Ley de Transparencia y Derecho de Acceso a la Información Pública.
Ley 2195 de 2022	Congreso de la República (Nacional)	Fortalece la integridad pública; sustenta el SIGRIP y los Programas de Transparencia y Ética Pública.
Decreto 1122 de 2024	Presidencia de la República / DAFP (Nacional)	Reglamenta la articulación del SIGRIP con MIPG y MECI.
Decreto 767 de 2022	Ministerio TIC (Nacional)	Define la estrategia de seguridad digital y su articulación con el Modelo MinTIC.
Resolución 500 de 2021	Ministerio TIC (Nacional)	Adopta los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).
Resolución 746 de 2022	Ministerio TIC (Nacional)	Actualiza y complementa los lineamientos del MSPI para entidades públicas.
Circular 007 de 2024	Consejería Distrital TIC – Bogotá D.C. (Distrital)	Define requisitos obligatorios para PETI distritales: accesibilidad WCAG 2.1 AA, interoperabilidad y seguridad digital.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Norma	Entidad que la expide / Ámbito	Descripción / Alcance
Guía para la Gestión Integral del Riesgo – Versión 7 (2025)	Departamento Administrativo de la Función Pública – DAFP (Nacional)	Referente metodológico para gestión integral del riesgo: COSO-ERM, apetito/tolerancia, madurez, riesgos de información, SIGRIP, KRI/KPI y reporte en MECI.
Decreto 612 de 2018	Presidencia / DAFP (Nacional)	Directrices para la integración de planes institucionales y estratégicos al Plan de Acción.
Decreto 1008 de 2018	Ministerio TIC (Nacional)	Lineamientos generales de la Política de Gobierno Digital; subroga capítulo del Decreto 1078/2015.
Guía para la administración del riesgo – Versión 6 (2022)	DAFP (Nacional)	Metodología oficial para administración del riesgo y diseño de controles (versión válida para 2022).
Guía DAFP v7 (2025)	DAFP (Nacional)	Metodología actualizada para administración integral del riesgo, apetito/tolerancia, madurez, KRI/KPI y reporte MECI.

Tabla 3 - Normatividad nacional y distrital

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

5.3. Guías técnicas

- **Guía DAFP v7 (2027)** para administración del riesgo y diseño de controles en entidades públicas.

5.4. Cumplimiento *Circular 007/2024*

Este apartado consolida las acciones, controles y evidencias que garantizan el cumplimiento de los lineamientos obligatorios de la Circular 007 de 2024 expedida por la Alta Consejería Distrital de TIC para los **Planes Estratégicos de Tecnologías de la Información (PETI)** distritales. Su propósito es asegurar la articulación con el **Plan de Tratamiento de Riesgos (PTRSPI)** y el **Sistema de Gestión de Seguridad de la Información (SGSI)**, entendiendo la accesibilidad como un componente crítico de la **disponibilidad** de la información.

5.4.1. Requisitos normativos exigidos

La Circular establece condiciones obligatorias para la planeación y operación de los PETI, que deben integrarse al ciclo **PHVA (Planear–Hacer–Verificar–Actuar)** del SGSI y ser **auditables** por entes de control internos y externos:

- **Accesibilidad digital** conforme a **WCAG 2.1 AA**
- **Interoperabilidad y trazabilidad del dato**
- **Seguridad de la información** bajo gobierno y control documental

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

5.4.2. Articulación con el PTRSPI

El PTRSPI incorpora estos lineamientos en sus capítulos normativos y operativos, vinculando:

- **Riesgos** asociados (p. ej., incumplimiento WCAG, interoperabilidad deficiente, brechas de seguridad)
- **Controles ISO/IEC 27002** aplicables (continuidad, acceso, nube, criptografía)
- **KPIs estratégicos** y metas verificables
- **Evidencias auditables** en repositorio SGSI con control de versiones conforme al **control 5.3 de ISO/IEC 27001:2022**

Requisito Circular 007/2024	Control / acción en PTRSPI	KPI y meta	Evidencia asociada	Referencia interna
Accesibilidad digital (WCAG 2.1 AA)	**Gestión del Riesgo de Disponibilidad**: Validación técnica de portales para eliminar barreras de acceso; incorporación de controles organizacionales y tecnológicos para garantizar el servicio a toda la población.	% conformidad AA ≥95%	Informes de validación de accesibilidad; actas de aprobación en comité; versión documental (5.3)	Cap. 7.1.3; Cap. 7.2; Cap. 10; Cumplimiento 007/2024

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Requisito Circular 007/2024	Control / acción en PTRSPI	KPI y meta	Evidencia asociada	Referencia interna
Interoperabilidad y trazabilidad del dato	Arquitectura habilitadora sobre nube híbrida, API Management y CDE; trazabilidad EO0203 ↔ PTRSPI	% activos clasificados ≥95%; % controles ISO ≥90%	Plan de implementación; matriz integrada; actas Mesa de trabajo SGSI (cuando exista) o CIGD; control 5.3	Cap. 3; Cap. 8; Cap. 9; Cap. 10
Seguridad de la información (SGSI operando)	Controles ISO/IEC 27002 priorizados: 5.30 continuidad, 8.2 acceso/MFA, 8.8 vulnerabilidades, 5.23 nube, 8.24 criptografía	% pruebas DRP exitosas ≥90%; % MFA ≥90%; % vulns en SLA ≥95%; % línea base cloud ≥90%; % cifrado ≥95%	Informes DRP; reporte plataforma MFA; escaneos y tickets; checklist línea base cloud; auditorías de cifrado	Cap. 7.2; Cap. 8.2; Cap. 10; Anexos 1–2
Control documental (ISO 27001, 5.3)	Versionamiento de políticas, SOA, anexos y cronograma operativo con folio y actas	% controles ISO implementados ≥90%	SOA actualizada; repositorio SGSI; actas de mesa de trabajo	Cap. 5; Cap. 8.2; Cap. 13; Anexo 4
PHVA y gobernanza	Plan de verificación y mejora continua; mapa de calor; flujo de	% riesgos críticos mitigados ≥90%; Nivel MSPI ≥4	Informes de auditoría; KPIs validados; actas y	Cap. 8.5; Cap. 10;

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Requisito Circular 007/2024	Control / acción en PTRSPI	KPI y meta	Evidencia asociada	Referencia interna
	retroalimentación con mesas de trabajo y actualización documentada		publicaciones en repositorio	Ilustraciones 1–2

Tabla 4 - Checklist de cumplimiento

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

6. Gobernanza del SGSI para el tratamiento del riesgo

El SGSI opera con un **modelo de doble instancia**:

- **Instancia de gobierno y decisión (Alta Dirección – Comité Institucional):** Aprueba políticas, el PTRSPI, la SOA y las **decisiones de riesgo** (aceptar, transferir, evitar, mitigar). Deja trazabilidad en **actas** y en el **repositorio SGSI** bajo **control documental 5.3**.
- **Instancias técnicas y operativas (Mesas de trabajo):**
    - *Mesa de trabajo SGSI*
    - *Mesa de trabajo operativa/táctica de TI*
    - *Mesa de gobierno de datos*

      Ejecutan la **operación del SGSI**, analizan riesgos, implementan controles y preparan **insumos técnicos** para decisión del Comité. Su creación y formalización está prevista y sustentada en la normatividad MinTIC citada en el documento.

Principio rector: Se separa la **decisión institucional** sobre el riesgo (gobierno) de la **implementación técnica** de controles (operación).

Evidencia y control documental: Toda actuación (políticas, SOA, anexos, cronogramas, informes, decisiones de riesgo) se **versiona** y **publica** en el repositorio SGSI con control 5.3, conforme ya definido en el PTRSPI.

Rol	Naturaleza	Responsabilidades clave	Propietario de activos / riesgos	Periodicidad de seguimiento	Instancia de decisión / escalamiento
Alta Dirección	Órgano de gobierno	Aprobar políticas, PTRSPI, SOA, criterios de aceptación/transferencia; asignar recursos; validar resultados del SGSI	Sí	Trimestral/Semestral	Comité Institucional (máxima instancia)
Comité Institucional	Instancia de decisión	Aprobar el PTRSPI, el apetito de riesgo y las decisiones de tratar el riesgo (aceptar, transferir, evitar, mitigar)	No	Trimestral/Semestral	Nivel 3 de escalamiento (máx. 72 h)
Dirección Administrativa y TIC	Dirección líder	Coordinar identificación, valoración y tratamiento; mantener evidencias y la publicación en el repositorio SGSI (5.3)	Sí	Mensual	Nivel 2 de escalamiento (máx. 48 h)

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Rol	Naturaleza	Responsabilidades clave	Propietario de activos / riesgos	Periodicidad de seguimiento	Instancia de decisión / escalamiento
Mesa de trabajo SGSI	Técnico-operativa	Consolidar inventarios, riesgos y controles; monitorear KPI/KRI; preparar informes para decisión del Comité; coordinar con otras mesas	No	Semanal/Mensual	Nivel 1 de escalamiento (máx. 24 h)
Mesa operativa/táctica de TI	Técnico-operativa	Ejecutar cambios, hardening, continuidad/DRP y operación de infraestructura; evidenciar resultados	No	Semanal/Mensual	Nivel 1 de escalamiento (máx. 24 h)
Mesa de gobierno de datos	Técnico-operativa	Definir lineamientos de datos, trazabilidad e interoperabilidad; articular con accesibilidad y seguridad	No	Mensual	Nivel 1 de escalamiento (máx. 24 h)
Propietarios de proceso	Gestión del riesgo	Identificar activos y riesgos; ejecutar controles en su ámbito; generar evidencias	Sí	Mensual	Nivel 1 → 2 → 3 según severidad

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Rol	Naturaleza	Responsabilidades clave	Propietario de activos / riesgos	Periodicidad de seguimiento	Instancia de decisión / escalamiento
Oficina Asesora Jurídica	Asesoría normativa	Validar requisitos legales/contractuales; revisar cláusulas con terceros	No	Trimestral	Participa como C/I
Control Interno	Aseguramiento	Auditar cumplimiento; emitir hallazgos y seguimiento; participar en PHVA	No	Trimestral/Semestral	Participa como I; reporta a Comité

Tabla 5 - Roles y responsabilidades

El tratamiento del riesgo se entiende como un proceso de decisión institucional, mientras que la implementación de controles corresponde a la ejecución técnica y operativa. Esta distinción permite separar claramente la responsabilidad por la aceptación del riesgo de la responsabilidad por la implementación de las medidas de control.

La creación de la **Mesa de Trabajo** de Seguridad de la Información (SGSI), de la **Mesa de Trabajo** Operativa/Táctica de TI y de la **Mesa de Trabajo** de Gobierno de Datos es obligatoria conforme al **Decreto 338 de 2022**, la **Resolución 746 de 2022** y la **Guía MGGTI.GE.ES.01 v3** del MinTIC, que exigen instancias formales de decisión, seguimiento y gobernanza en materia de tecnología, seguridad digital y datos. Estas **mesas de trabajo** no existen actualmente; por ello, su creación será sometida a la aprobación del **Comité Institucional de Gestión y Desempeño** el **3 de marzo de 2026**.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Actividad	Comité Institucional	Dirección Adm. y TIC	Mesa SGSI	Mesa TI	Mesa Datos	Seguridad	Infraestructura	Jurídica	Propietarios de proceso	Control interno
Identificación de riesgos	I	A	R	C	C	C	C	I	R	I
Valoración y priorización	I	A	R	C	C	C	C	I	C	I
Definición de controles	I	A	R	R	C	C	C	C	C	I
Implementación de controles	I	A	R	R	C	R	R	C	C	I
Monitoreo de KPI/KRI	I	C	R	R	C	R	R	I	I	R
Actualización de políticas/SOA	A	R	C	C	C	C	I	C	I	I

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Actividad	Comité Institucional	Dirección Adm. y TIC	Mesa SGSI	Mesa TI	Mesa Datos	Seguridad	Infraestructura	Jurídica	Propietarios de proceso	Control interno
Incorporación de riesgos al mapa institucional	A	R	C	C	C	C	I	I	C	I
Aprobación del PTRSPI	A	R	C	C	C	I	I	I	I	I
Auditoría interna del SGSI	A (recepción de informes)	C	I	I	I	C	I	I	I	R

Tabla 6 - Matriz RACI

6.1. Flujo de escalamiento para riesgos no mitigados e incidentes críticos

- **Nivel 1 – Operación (máx. 24 horas):** Mesa de trabajo SGSI coordina con Mesa operativa de TI y Mesa de gobierno de datos; consolida análisis y medidas inmediatas; registra evidencia técnica y minuta de la mesa.

- **Nivel 2 – Dirección (máx. 48 horas):** Dirección Administrativa y TIC decide medidas transitorias, asigna recursos y ordena acciones correctivas; eleva recomendación al Comité.
- **Nivel 3 – Gobierno (máx. 72 horas):** Comité Institucional aprueba decisiones de riesgo (aceptar, transferir, evitar, mitigar) y define orientaciones estratégicas; deja acta y control de versiones (5.3).

  Evidencia: Actas y registros en Anexo 2.

  Referencia normativa: ISO 27001 cl. 6.1.3, 8.2; MinTIC LI.GS.02.

6.2. Mapa de actores externos para transferencia de riesgos

- Proveedores críticos (ERP JSP7, nube híbrida) → Contratos con cláusulas de continuidad y seguridad digital.
- Aseguradoras → Pólizas para riesgos residuales (ciberseguridad, continuidad).

  Evidencia: Contratos y pólizas archivadas en Anexo 2.

  Referencia normativa: ISO 27002 control 5.19; MinTIC LI.ST.04.

Gobernanza aplicada:

- *Mesas de trabajo* gestionan la **verificación técnica** (checklists, evidencias, pruebas) y reportan recomendaciones.
- *Dirección TIC* consolida resultados y condiciones contractuales.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

- **Comité Institucional aprueba** la estrategia de **transferencia de riesgos** y sus límites (apetito y tolerancia), dejando acta y registro en repositorio SGSI (5.3).

6.3. Reglas de control documental y defendibilidad

- **Control 5.3 (ISO/IEC 27001):** Todas las decisiones, informes, políticas, SOA y anexos del SGSI se **versionan** y **publican** en el repositorio oficial del SGSI como **fuente única de verdad**.
- **Evidencia operativa:** Informes DRP, reportes MFA, escaneos y tickets de vulnerabilidades, auditorías de configuración cloud, validaciones WCAG 2.1 AA, entre otras evidencias ya definidas en el plan.
- **Ciclo PHVA:** Las mesas soportan “Planear–Hacer–Verificar–Actuar”; el Comité realiza la **revisión por la dirección** y aprueba mejoras.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

7. Desarrollo

El desarrollo del ***PTRSPI*** 2026–2029 se fundamenta en los resultados del diagnóstico institucional, las recomendaciones de entes de control y la sincronización con las fases metodológicas del ***PETI*** definidas por ***MinTIC*** (Planear–Analizar–Construir–Socializar). **El método considera la evaluación del nivel de madurez y el apetito de riesgo institucional, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025), como insumo para la priorización y toma de decisiones estratégicas.** Este bloque articula el análisis de brechas, la priorización de riesgos, la definición de controles y la gobernanza, asegurando defendibilidad ante auditoría y coherencia con la transformación digital.

7.1. Diagnóstico actual

El diagnóstico se consolida a partir de **insumos institucionales y normativos verificables**, con el propósito de **priorizar riesgos críticos**, **definir controles**, **establecer KPIs** y garantizar **trazabilidad con el SGSI** y los instrumentos estratégicos de la Entidad. Las fuentes principales son:

- **Autodiagnósticos de Gobierno Digital y Seguridad Digital 2025**, junto con las **brechas FURAG**, integradas en el PETI mediante anexos específicos. Estas se adoptan como **evidencia fuente** para la priorización de riesgos y actividades del PTRSPI.
- **Hallazgos de auditorías internas 2024** y planes de mejoramiento vigentes, que orientan la incorporación de riesgos al **mapa institucional** y la planificación de **transferencia o compartición de riesgos**.

- **Matriz GAP ISO/IEC 27001:2022 vs MSPI vs situación actual**, que identifica el **estado de implementación**, las **evidencias críticas** y los riesgos asociados a **continuidad**, **vulnerabilidades**, **accesos** y **cifrado**.
- **Circular 007 de 2024**, como requisito distrital para **accesibilidad digital (WCAG 2.1 AA)**, **interoperabilidad** y **seguridad del PETI**, cuyo cumplimiento debe reflejarse en el PTRSPI como **riesgo**, **control** y **evidencia verificable** bajo el ciclo **PHVA**.

7.1.1. Síntesis de hallazgos críticos y coherencia con PETI – PSPI

El diagnóstico confirma **cinco riesgos críticos** que impactan continuidad, protección de datos y resiliencia tecnológica; todos cuentan con controles ISO/IEC 27002, KPIs y evidencias esperadas en el PTRSPI:

- **Indisponibilidad de servicios críticos**, con necesidad de elevar RTO/RPO y formalizar pruebas DRP periódicas con evidencia técnica.
- **Compromiso de cuentas de correo** por cobertura insuficiente de **MFA**; meta de activación ≥90%.
- **Vulnerabilidades críticas** en portal y cargas cloud; se requiere asegurar SLAs de remediación y trazabilidad en tickets e informes de escaneo.
- **Configuración insegura en servicios en la nube** (permisos excesivos/exposición pública); demanda línea base de seguridad cloud, hardening y auditorías periódicas.
- **Datos sin cifrado en tránsito o reposo**; política y despliegue de criptografía en estado parcial/no iniciado con meta ≥95% de cobertura técnica (TLS, repositorios y respaldos).

La dirección estratégica del **PETI** (nube híbrida, **API Management** y **CDE**) es el habilitador técnico del tratamiento de riesgos del PTRSPI, alineado con el objetivo **EO0203** y con la gobernanza del SGSI (actas,

control de versiones), asegurando interoperabilidad y trazabilidad del dato en la toma de decisiones. El **PSPI** agrega KPIs estratégicos (MTTD, MTTR, % MFA, % cifrado, % pruebas DRP exitosas), que se adoptan como medidas de desempeño y umbrales correctivos en el PTRSPI bajo **PHVA**.

7.1.2. Consolidado de hallazgos ↔ riesgo ↔ control ↔ kpi ↔ evidencia ↔ gobernanza

Propósito: Integrar en una sola vista los hallazgos fuente (PETI/PSPI/GAP/Auditoría), su traducción a riesgos del PTRSPI, controles ISO/IEC 27002 aplicables, KPIs y metas, evidencias auditables, fase MinTIC y roles responsables (RACI). El detalle operativo (fechas, minutas, asistentes) se conserva en **"Plan de Acción proceso gestión de TI 2026.xlsx"** y en los **Anexos del SGSI** para evitar duplicidad.

Hallazgo fuente (PETI/PSPI/GAP/Auditoría)	Riesgo PTRSPI (ID)	Control ISO/IEC 27002	KPI y meta	Evidencia auditable	Fase MinTIC	Responsable
Pruebas DRP parciales; RTO/RPO sin verificación periódica	R01: Indisponibilidad de servicios críticos	5.30 Continuidad del negocio	% pruebas de restauración exitosas ≥90%	Informe DRP + acta Mesa de Trabajo SGSI (cuando	Construir	Infraestructura TI

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Hallazgo fuente (PETI/PSPI/GAP/Auditoría)	Riesgo PTRSPI (ID)	Control ISO/IEC 27002	KPI y meta	Evidencia auditable	Fase MinTIC	Responsable
				exista) o CIGD		
Cobertura MFA insuficiente en correo institucional	R02: Compromiso de cuentas de correo	8.2 Control de acceso	% cuentas con MFA ≥90%	Reporte de plataforma MFA	Construir	Gestión TIC
Vulnerabilidades sin remediación dentro de SLA (web/cloud)	R03/R06: Vulnerabilidades críticas	8.8 Gestión de vulnerabilidades	% vulnerabilidades corregidas en SLA ≥95%	Informes de escaneo + tickets de remediación	Analizar/Construir	Seguridad
Configuraciones inseguras en servicios cloud (permisos/exposición)	R04: Configuración insegura cloud	5.23 Seguridad en servicios en la nube	% cumplimiento línea base cloud ≥90%	Checklist línea base cloud + auditoría de	Construir	Seguridad de la información

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Hallazgo fuente (PETI/PSPI/GAP/Auditoría)	Riesgo PTRSPI (ID)	Control ISO/IEC 27002	KPI y meta	Evidencia auditable	Fase MinTIC	Responsable
				configuración		
Ausencia/insuficiencia de cifrado en tránsito y reposo	R05: Datos sin cifrado	8.24 Criptografía	% cifrado en tránsito y reposo ≥95%	Informes TLS/cifrado + respaldo cifrado	Construir	Seguridad de la información
Exigencia distrital de accesibilidad digital (Circular 007/2024)	R08 (nuevo): incumplimiento WCAG 2.1 AA	5.x/8.x controles organizacionales y tecnológicos aplicables	% conformidad AA ≥95%	Informes de validación de accesibilidad + actas de aprobación	Planear/Construir	Dirección TIC + Comunicaciones

Tabla 7 - Tabla ejecutiva consolidada: hallazgo ↔ riesgo ↔ control ↔ kpi ↔ evidencia ↔ gobernanza

7.1.3. Fuentes, anexos y trazabilidad metodológica

Propósito: Conectar cada fuente diagnóstica con el repositorio SGSI, la fase MinTIC y el tipo de evidencia, manteniendo una sola "fuente de verdad" para seguimiento y auditoría.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Fuente diagnóstica	Ubicación/Repositorio SGSI	Fase MinTIC	Tipo de evidencia
Autodiagnósticos Gobierno Digital y Seguridad Digital 2025 (PETI)	Anexos PETI (Autodiagnósticos y resultados)	Analizar	Informe y resultados oficiales
Brechas FURAG (PETI)	Anexos PETI (Brechas y plan de acciones)	Analizar	Matriz de brechas FURAG
Matriz GAP ISO/MSPI (PTRSPI)	Capítulo 7.2 GAP y Anexo correspondiente	Analizar	Matriz con estado y evidencias críticas
Hallazgos auditoría interna 2024	Repositorio SGSI (informes y planes de mejora)	Verificar	Informes y actas de seguimiento
Circular 007/2024 (accesibilidad y seguridad)	Capítulos normativos PETI/PSPI y evidencias de pruebas	Planear/Construir	Lineamientos y reportes de conformidad
Cronograma operativo 2026 (Plan de Acción TI)	“Plan de Acción proceso gestión de TI 2026.xlsx”	Construir	Fechas, responsables y entregables oficiales
Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025)	Capítulo 5 (Normatividad) y Capítulo 7 (Metodología) del PTRSPI; repositorio SGSI	Planear / Analizar	Documento oficial DAFP v7; acta de adopción en CIGD (actual) o el Comité Institucional de Gestión y

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Fuente diagnóstica	Ubicación/Repositorio SGSI	Fase MinTIC	Tipo de evidencia
			Desempeño (CIGD) (proyectado); matriz de madurez y apetito de riesgo

Tabla 8 - Tabla de fuentes, anexos y trazabilidad metodológica

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

7.2. Informe GAP – ISO / IEC 27001:2022 vs MSPI vs Situación actual

El **Informe GAP** se estructura en dos **vistas complementarias** para asegurar **defendibilidad ante auditoría** y **trazabilidad normativa**: una matriz **resumida en este capítulo**, que integra dimensiones críticas (cláusulas de **ISO/IEC 27001:2022**, controles de **ISO/IEC 27002:2022**, estado y porcentaje de cumplimiento, riesgo SGSI asociado, KPI y meta homologada, evidencia auditable, acción **PHVA** y fase **MinTIC**), y una **matriz detallada** en el Anexo 2: Matriz de trazabilidad de riesgos con granularidad operativa (actividad, **RACI**, umbrales y acciones, dependencias/ANS, riesgo residual y observaciones de auditoría).

ISO 27001:2022 (cláusula / control)	MSPI (lineamiento)	Estado	% Cumpl.	Riesgo SGSI asociado	ISO/IEC 27002 (control)	KPI (línea base → meta)	Umbral / acción	PHVA	Fase MinTIC	Evidencia / Gobernanza	RACI (R / A / C / I)
5.30 Continuidad (operación)	ST.04 Continuidad; ST.11 Respaldo	Parcial	54%	Indisponibilidad de servicios	5.30 Continuidad	% pruebas DRP (70% → ≥90%)	<70% → activar plan de contingencia y escalar a CIGD (actual) Mesa de Trabajo SGSI (proyectado)	H/V/A	Construir	Informes DRP + actas Mesa de Trabajo SGSI (cuando exista) o CIGD	Infraestructura (R) / CIGD o Mesa de Trabajo SGSI (A) / Seguridad (C) / Control Interno (I)

ISO 27001:2022 (cláusula / control)	MSPI (lineamiento)	Estado	% Cumpl.	Riesgo SGSI asociado	ISO/IEC 27002 (control)	KPI (línea base → meta)	Umbral / acción	PHVA	Fase MinTIC	Evidencia / Gobernanza	RACI (R / A / C / I)
8.2 Control de acceso (MFA)	Seguridad digital	Parcial	N/D	Compromiso de cuentas / privilegios	8.2 Control de acceso	% MFA (62% → ≥90%)	<75% → campaña de activación y bloqueo cuentas sin MFA	H/V/A	Construir	Reporte plataforma MFA	Gestión TIC (R) / CIGD o Mesa de Trabajo SGSI (A) / Seguridad (C) / Control Interno (I)
8.8 Gestión de vulnerabilidades	Ciberseguridad	Parcial	N/D	Explotación de vulnerabilidades	8.8 Vulnerabilidades	% corregidas en SLA (54% → ≥95%)	<80% → ajustar ciclo escaneo→remediación y SLAs	P/H/V/A	Analizar/Construir	Informes escaneo + tickets + SLAs	Seguridad (R) / CIGD o Mesa de Trabajo SGSI (A) / Infraestructura (C) / Control Interno (I)

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

ISO 27001:2022 (cláusula / control)	MSPI (lineamiento)	Estado	% Cumpl.	Riesgo SGSI asociado	ISO/IEC 27002 (control)	KPI (línea base → meta)	Umbral / acción	PHVA	Fase MinTIC	Evidencia / Gobernanza	RACI (R / A / C / I)
8.24 Criptografía (política y controles)	Seguridad tecnológica	No iniciado/Parcial	30%	Exposición de datos / sanciones PII	8.24 Criptografía	% cifrado (40% → ≥95%)	<80% → implementar política y despliegue técnico (TLS/reposo)	P/H/V/A	Construir	Informes TLS / backup cifrado + auditoría	Seguridad info (R) / CIGD o Mesa de Trabajo SGSI (A) / Infraestructura (C) / Jurídica (I)
5.23 Seguridad en servicios en la nube	Nube	Parcial	N/D	Permisos excesivos / exposición pública	5.23 Cloud security	% cumplimiento línea base cloud (50% → ≥90%)	<70% → aplicar baseline/hardening y auditoría de configuración	P/H/V/A	Construir	Checklist baseline cloud + auditoría de configuración	Seguridad info (R) / CIGD o Mesa de Trabajo SGSI (A) / Infraestructura (C) / Proveedor (I)

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

ISO 27001:2022 (cláusula / control)	MSPI (lineamiento)	Estado	% Cumpl.	Riesgo SGSI asociado	ISO/IEC 27002 (control)	KPI (línea base → meta)	Umbral / acción	PHVA	Fase MinTIC	Evidencia / Gobernanza	RACI (R / A / C / I)
Accesibilidad (Circular 007/2024)	Gobierno Digital	Parcial	N/D	Incumplimiento WCAG 2.1 AA	5.x/8.x org./tec.	% conformidad AA (N/D → ≥95%)	<95% → plan de adecuación y nueva validación	P/H/V/A	Planear/Construir	Informes de validación AA + actas + control 5.3	Dirección TIC (R) / Comité Institucional (A) / Comunicaciones (C) / Control Interno (I)
6.1.3 Tratamiento del riesgo / 5.3 Control documental	Gestión de riesgos	Parcial	N/D	Trazabilidad de riesgos priorizados en mapa institucional	5.30, 8.2, 8.8, 5.23, 8.24 (según riesgo)	% riesgos críticos del PTRSPI cargados al mapa institucional (100%)	<100% al corte trimestral → Escalar a CIGD/Comité Institucional y activar plan de cierre	P/H/V/A	Construir/Socializar	Acta CIGD/SGSI + registro en matriz institucional + publicación en repositorio SGSI (5.3)	Dirección TIC (R) / CIGD (A) / Seguridad TI (C) / Control Interno (I)

Tabla 9 - Matriz GAP: ISO 27001:2022 vs MSPI vs Situación actual

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Nota metodológica: Utiliza los criterios de **estado de implementación** *(Implementado / Parcial / No iniciado / N/D)*, **% de cumplimiento** ponderado por evidencia crítica.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

7.3. Desarrollo metodológico

La administración de riesgos de **seguridad y privacidad de la información** se implementa mediante un **método reproducible y auditable**, diseñado para garantizar **trazabilidad normativa**, **coherencia metodológica** y **defendibilidad ante auditoría**. Este método integra las siguientes etapas:

- **Identificación de activos y riesgos**
- **Valoración del riesgo** mediante la fórmula *Impacto × Probabilidad*
- **Definición y operación de controles**
- **Tratamiento del riesgo** (mitigar, transferir, evitar o aceptar)

El enfoque se encuentra alineado con:

- **Guía DAFP v7 (2025)**
- **ISO/IEC 27001:2022** (cláusulas 6.1.2 y 6.1.3)
- Ciclo **PHVA (Planear–Hacer–Verificar–Actuar)**
- Fases **MinTIC del PETI** (*Planear–Analizar–Construir–Socializar*)

Estas referencias aseguran la integración con los instrumentos estratégicos y la mejora continua del **SGSI**.

Además, por exigencia distrital, se incorpora la **Circular 007 de 2024** (accesibilidad **WCAG 2.1 AA**, interoperabilidad y seguridad) como requisito verificable en el marco metodológico y como **riesgo/control** sujeto a evidencia y aprobación en comité (control 5.3 de ISO/IEC 27001:2022).

7.3.1. Fase 1: Identificación de los activos de seguridad de la información

Propósito: Construir y mantener el inventario de activos por proceso, clasificar la información, determinar criticidad y asociar riesgos inherentes (**confidencialidad, integridad, disponibilidad**), incluyendo el componente regulatorio de **accesibilidad digital** en portales y aplicaciones de cara al ciudadano.

La clasificación y criticidad se alinean con la metodología de la **Guía v7 (2025)**, incorporando la **evaluación del nivel de madurez del proceso** como insumo para priorización y toma de decisiones estratégicas.

7.3.1.1. Pasos mínimos

- **Inventario de activos:** Listar los activos por proceso, identificar el propietario, clasificar activos e información y determinar la criticidad (incluyendo infraestructura crítica cibernética).
- **Asociación de riesgos:** Vincular riesgos inherentes (CID) por activo, analizando amenazas y vulnerabilidades que puedan materializarlos, registrando la información en la **matriz institucional de riesgos del SGSI**.
- **Accesibilidad digital:** Incorporar el riesgo de accesibilidad (**WCAG 2.1 AA**) como riesgo transversal en sistemas y portales, definiendo controles y evidencias de validación técnica, con aprobación en comité conforme al **control 5.3 de ISO/IEC 27001:2022**.

7.3.1.2. Entregables y evidencias

- Inventario de activos por proceso (propietario, clasificación, criticidad)
- Matriz de riesgos actualizada
- Actas del Mesa de Trabajo SGSI de Gestión y Desempeño – CIGD con control de versiones (5.3)
- Publicación en el repositorio SGSI como fuente única de verdad documental

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

7.3.1.3. Trazabilidad EO0203–PTRSPI

Las actividades de esta fase se articulan con el Capítulo 8 – Plan de implementación, materializando el objetivo estratégico EO0203 mediante la modernización de la infraestructura sobre nube híbrida, API Management y Centro de Datos Empresarial (CDE). Esta integración habilita interoperabilidad y trazabilidad del dato bajo gobernanza del Mesa de Trabajo SGSI de Gestión y Desempeño – CIGD (control 5.3).

La contribución se mide mediante metas asociadas a los controles ISO/IEC 27002:

- **Continuidad del negocio (5.30)**
- **Control de acceso (8.2)**
- **Gestión de vulnerabilidades (8.8)**
- **Seguridad en la nube (5.23)**
- **Criptografía (8.24)**

Estos indicadores se articulan con los **KPIs del Capítulo 10** y la operación del ciclo **PHVA**.

7.3.2. Fase 1.1: Identificación del riesgo

Propósito: Determinar el **nivel de riesgo** con la fórmula: **Nivel de riesgo = Impacto × Probabilidad** y clasificarlo para orientar el tratamiento.

Parámetros: Impacto (1 mínimo, 5 crítico) y Probabilidad (1 improbable, 5 muy probable).

Puntaje	Clasificación
1–5	Bajo
6–10	Moderado
11–15	Alto
16–25	Extremo

Tabla 10 - Valoración del riesgo

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Los valores se asignan conforme a Guía DAFP v7 (2025) y se registran en la matriz de riesgos institucional; cada cálculo debe quedar documentado en el formato oficial del SGSI y validado por el Mesa de Trabajo SGSI (ISO/IEC 27001:2022, cl. 6.1.2–6.1.3).

La valoración se ajusta a los **criterios de apetito, tolerancia y capacidad de riesgo** definidos en la Guía v7, vinculando estos parámetros a la gobernanza institucional y al ciclo PHVA.

7.3.3. Fase 2: Valoración del riesgo

7.3.3.1. Propósito

Operar **controles ISO/IEC 27002:2022** sobre riesgos **moderados–extremos**, integrando **KPIs**, **evidencias auditables** y **gobernanza en comité**. La **priorización** proviene del diagnóstico y del **Informe GAP** en las dimensiones de **continuidad, control de acceso, vulnerabilidades, seguridad en la nube, criptografía y accesibilidad**.

7.3.3.2. Controles prioritarios (ejemplos)

- Continuidad del negocio (5.30): pruebas DRP periódicas sobre servicios críticos (ERP/JSP7, correo institucional, SGDEA/TAMPUS), verificación de RTO/RPO y evidencia técnica en informes y actas de Mesa de Trabajo SGSI.
- **Control de acceso (8.2):** cobertura **MFA** ≥90% en cuentas de correo y servicios críticos; política de credenciales y reportes de la plataforma de MFA como evidencia.
- **Gestión de vulnerabilidades (8.8):** ciclo escaneo → remediación con **SLAs**, trazabilidad en tickets e informes de escaneo para web y cargas cloud.
- **Seguridad en servicios en la nube (5.23):** línea base de seguridad cloud, hardening, logging, segmentación, y auditorías de configuración (checklist + informe).
- **Criptografía (8.24):** cifrado en tránsito (**TLS**) y en reposo (BD/backup) con cobertura ≥95%; evidencia de configuración, auditoría y respaldo cifrado.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

- **Accesibilidad (Circular 007/2024):** conformidad **WCAG 2.1 AA** ≥95% en portales/sistemas, con informes de validación y actas de aprobación en comité (control 5.3).

7.3.3.3. Evidencias esperadas

Informes **DRP** y de **backup**, reportes **MFA**, escaneos/tickets/SLAs, auditorías de configuración **cloud** y validaciones **WCAG 2.1 AA**; todas **versionadas** y **publicadas** en el **repositorio SGSI** bajo **control de versiones 5.3**.

7.3.3.4. Alineación con PETI y gobernanza del SGSI.

La sincronización EO0203–PTRSPI asegura que la modernización tecnológica del PETI 2026–2029 (nube híbrida, API Management, CDE) se traduzca en controles ISO/IEC 27002 operativos, KPIs verificables y evidencias auditables (actas, SOA, repositorio con control 5.3).
El detalle de actividades y responsables se encuentra en el Capítulo 8 y en el Plan de Acción 2026, como fuente única para auditoría, con trazabilidad a actas del Mesa de Trabajo SGSI de Gestión y Desempeño – CIGD.

7.3.4. Fase 3: Definición y operación de controles

Propósito: Definir y ejecutar controles para mitigar riesgos altos y extremos, transferir riesgos residuales, evitar riesgos no aceptables y aceptar riesgos dentro del apetito aprobado (Guía v7).

Ajuste COSO-ERM: Se incorpora el principio de “tono desde la cima” (Tone at the Top) como parte de la gobernanza, asegurando que las decisiones de aceptación o transferencia de riesgos sean aprobadas por la **Alta Dirección** y documentadas en actas del Comité Institucional, conforme a **ISO/IEC 27001:2022** cl. 6.1.3 y al ciclo **PHVA del SGSI**.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Opciones: Mitigar (controles), **Transferir** (seguros/contratos/servicios), **Evitar** (cambio de proceso) o **Aceptar** (residual dentro del apetito). Toda decisión debe **documentarse y aprobarse** por el **propietario del riesgo** y por la **Alta Dirección** (actas y control de versiones).

Criterios de aceptación (umbrales):

Clasificación	Puntaje	Decisión
Bajo	1–5	Aceptable sin tratamiento adicional
Moderado	6–10	Mitigar con controles preventivos
Alto	11–15	Mitigar obligatoriamente; considerar transferencia
Extremo	16–25	Mitigar + DRP; no se acepta residual

Tabla 11 - Criterios de aceptación

La **aceptación** de riesgos altos y extremos, así como la **transferencia/evitación** de riesgos residuales, es **responsabilidad exclusiva** de la **Alta Dirección** y debe quedar evidenciada en **actas** del Comité Institucional (***ISO*** / ***IEC 27001:2022***, cl. 6.1.3).

7.3.4.1. Condiciones para aceptación

- Toda decisión debe documentarse en el formato “Aprobación de tratamiento de riesgo”.
- Debe ser firmada por el propietario del riesgo y validada por Alta Dirección.
- La aceptación de riesgos altos y extremos, así como la decisión de transferir o evitar riesgos residuales, es responsabilidad exclusiva de la Alta Dirección y debe quedar evidenciada en actas del Comité Institucional de Gestión y Desempeño.

Evidencia: Acta del Comité Institucional que aprueba el apetito de riesgo y los umbrales.

Referencia normativa: ISO/IEC 27001:2022 cl. 6.1.3; MinTIC LI.GS.02.

7.3.5. Articulación con *PETI*, *PSPI* y fases *MinTIC*

El método se **sincroniza** con las fases **MinTIC del PETI (Planear–Analizar–Construir–Socializar)** para evitar reprocesos y sostener defendibilidad metodológica, manteniendo la trazabilidad entre diagnóstico, brechas **FURAG**, cronograma y anexos técnicos.

Se garantiza coherencia con el **objetivo EO0203** (infraestructura de última generación sobre **nube híbrida**, **API Management** y **CDE**) como habilitadores técnicos de la gestión de riesgos del PTRSPI, y con los **KPIs** definidos en el **PSPI** (MTTD, MTTR, % MFA, % cifrado, % pruebas DRP exitosas) que se adoptan como medidas de desempeño y umbrales correctivos bajo ***PHVA***.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

7.3.6. Articulación de anexos con fases MinTIC

Para garantizar trazabilidad metodológica y defendibilidad ante auditoría, los anexos del PTRSPI se articulan explícitamente con las fases definidas por MinTIC para los PETI (**Planear–Analizar–Construir–Socializar**). Esta integración evita duplicidades y asegura que cada anexo refuerce los contenidos desarrollados en el documento base.

Fase MinTIC	Anexo vinculado	Contenido clave	Evidencia esperada
Planear	Anexo 3: Autodiagnósticos 2025	Resumen ejecutivo de autodiagnósticos de Gobierno Digital y Seguridad Digital	Informe oficial, acta de validación
Analizar	Anexo 3: Brechas FURAG	Matriz de brechas priorizadas y acciones correctivas	Matriz FURAG, acta Mesa de Trabajo SGSI (cuando exista) o CIGD
Construir	Anexo 4: Plan de Acción 2026.xlsx	Cronograma detallado (actividades, fechas, responsables, entregables) con control documental 5.3	Archivo versionado en repositorio SGSI
Socializar	Anexo 2: Actas y matriz de trazabilidad	Actas de Mesa de Trabajo SGSI (cuando exista) o CIGD e Institucional, matriz integrada de riesgos y controles	Actas firmadas, matriz actualizada

Tabla 12 - Articulación de anexos con fases del MinTIC

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

8. Plan de implementación

El **Plan de implementación** operacionaliza el **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** mediante una ejecución **ordenada, trazable y defendible**, sustentada en los **diagnósticos institucionales**, el **Informe GAP** y las **prioridades estratégicas del PETI y del PSPI**, en coherencia con **ISO/IEC 27001:2022**, **ISO/IEC 27002:2022**, el **MSPI** y la **Circular 007 de 2024**.

El plan se rige por principios de **gobernanza** y **mejora continua (PHVA)**, articulando cada actividad con:

- El **control ISO/IEC 27002** aplicable
- El **objetivo estratégico del PETI (OE-TI)**
- El **KPI** del **PSPI**
- Las **fases MinTIC** (*Planear–Analizar–Construir–Socializar*)
- La **evidencia auditable** publicada en el **repositorio SGSI** con **control de versiones (5.3)**

El **detalle operativo** (cronograma, responsables, minutas y entregables) se gestiona en el documento **"Plan de Acción proceso gestión de TI 2026.xlsx"**.

8.1. Principios de implementación

- **Alineación estratégica**: La ejecución se articula con las metas del PETI (nube híbrida, API Management y CDE) para habilitar interoperabilidad y trazabilidad del dato (objetivo **EO0203**).
- **Cumplimiento distrital**: La **Circular 007 de 2024** se integra como requisito verificable de **accesibilidad (WCAG 2.1 AA)**, interoperabilidad y seguridad, evidenciado en comités y control de versiones.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

- Gobernanza y PHVA: Validación en Mesa de Trabajo SGSI/Institucional, evidencias en actas y ciclo Planear–Hacer–Verificar–Actuar con indicadores y acciones correctivas.
- **Coherencia con el diagnóstico y el GAP**: Cierre de brechas priorizadas en continuidad (**DRP**), **MFA**, **vulnerabilidades**, **seguridad en nube**, **criptografía** y **accesibilidad** conforme a capítulos 7.1 y 7.2.

8.2. Matriz de actividades

La matriz resume las actividades críticas. El cronograma (fechas, hitos, dependencias) y los detalles de ejecución se mantienen en **"Plan de Acción proceso gestión de TI 2026.xlsx"** y en **Anexos SGSI** para evitar duplicidades y sostener defendibilidad documental.

Actividad	Control ISO/IEC 27002	OE-TI / KPI	Meta	Evidencia auditable	Fase MinTIC	Responsable
Validar pruebas DRP en servicios críticos (ERP/JSP7, correo, SGDEA/TAMPUS) incluyendo RTO/RPO	5.30 Continuidad	OE-TI 3 / % pruebas exitosas	≥90%	Informe DRP + acta Mesa de Trabajo SGSI (cuando exista) o CIGD	Construir	Infraestructura TI
Activar MFA en cuentas	8.2 Control de acceso	OE-TI 3 / % MFA	≥90%	Reporte plataforma MFA	Construir	Gestión TIC

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Actividad	Control ISO/IEC 27002	OE-TI / KPI	Meta	Evidencia auditable	Fase MinTIC	Responsable
institucionales y servicios críticos						
Operar ciclo escaneo→remediación de vulnerabilidades con SLAs y trazabilidad en tickets (web/cloud)	8.8 Gestión de vulnerabilidades	OE-TI 3 / % corregidas en SLA	≥95%	Informes de escaneo + tickets + SLAs	Analizar/Construir	Seguridad
Definir y aplicar línea base de seguridad cloud (hardening, logging, segmentación), con auditoría de configuración	5.23 Seguridad en nube	OE-TI 3 / % cumplimiento baseline	≥90%	Checklist baseline + informe auditoría	Construir	Seguridad de la información
Implementar cifrado en tránsito (TLS) y en reposo (BD/backup)	8.24 Criptografía	OE-TI 3 / % cifrado	≥95%	Informes TLS/cifrado + respaldo cifrado	Construir	Seguridad de la información

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Actividad	Control ISO/IEC 27002	OE-TI / KPI	Meta	Evidencia auditable	Fase MinTIC	Responsable
Ejecutar validaciones de accesibilidad (WCAG 2.1 AA) en portales/sistemas y registrar correcciones	5.x/8.x org./tec.	OE-TI 4 / % conformidad AA	≥95%	Informes de validación AA + actas de aprobación	Planear/Construir	Dirección TIC + Comunicaciones
Ajustar SOA y políticas; registrar control de versiones (5.3) y decisiones en actas	5.3 Control documental	OE-TI 4 / % controles ISO implementados	≥90%	SOA actualizada + actas Mesa de Trabajo SGSI (cuando exista) o CIGD	Planear	Dirección TIC / Mesa de Trabajo SGSI (cuando exista) o CIGD
Fortalecer ANS y pruebas de continuidad SaaS con proveedores críticos	5.19 Relación con partes externas + 5.30	OE-TI 3 / % continuidad SaaS	≥90%	Actas de pruebas + ANS de proveedor	Construir	Infraestructura / Gestión de proveedores

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Actividad	Control ISO/IEC 27002	OE-TI / KPI	Meta	Evidencia auditable	Fase MinTIC	Responsable
Incorporar riesgos críticos del PTRSPI al mapa de riesgos institucional conforme a metodología DAFP v7	6.1.3 Tratamiento del riesgo / 5.3 Control documental	OETI 3 / % riesgos críticos incorporados al mapa institucional	100% al Q4/2026	Acta de Comité (Mesa de Trabajo SGSI (cuando exista) o CIGD) + registro en mapa institucional + publicación en repositorio SGSI (control 5.3)	Construir / Socializar	Dirección TIC (R), CIGD (A), Seguridad TI (C), Control Interno (I)

Tabla 13 - Resumen de actividades

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

8.3. Trazabilidad normativa y contractual por actividad

La siguiente matriz consolida la trazabilidad normativa y contractual de cada actividad del PTRSPI, integrando:

- Controles aplicables de ISO/IEC 27001:2022 (cláusula y control)
- Controles específicos del Anexo A de ISO/IEC 27002:2022
- Lineamientos del Modelo de Seguridad y Privacidad de la Información – MinTIC (Resolución 500/2021, Decreto 767/2022)
- Cláusulas contractuales del contrato estatal vigente (número y descripción)
- KPIs estratégicos, evidencias auditables y responsables

Esta matriz reemplaza las tablas previas para evitar duplicidad y fortalecer la defendibilidad ante auditoría externa ISO 27001 y entes de control.

Nota:

El detalle operativo (cronograma, formatos, asistentes, minutas) y las evidencias específicas se mantienen en el Anexo 2: Matriz de trazabilidad de riesgos como repositorio auditable y fuente oficial.

Toda decisión sobre aceptación, transferencia o mitigación de riesgos debe estar documentada en actas del Comité Institucional de Gestión y Desempeño (CIGD) y del Comité Institucional, archivadas en el Anexo.

8.4. Plan de contingencia y relación con DRP

El **PTRSPI** establece la referencia normativa y contractual al **Plan de Recuperación Tecnológica ante Desastres (DRP)**, documento independiente que desarrolla en detalle las **estrategias y procedimientos**

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

para garantizar la continuidad de los servicios críticos.

El **DRP** se encuentra alineado con:

- **ISO/IEC 27001:2022** (cláusulas 8 y 9.1)
- **Control 5.30** (continuidad del negocio)
- Lineamientos del **MSPI del MinTIC**

Para detalles operativos y cronograma de pruebas, consulte el **Anexo correspondiente** o el **DRP en el repositorio SGSI**.

En 2025 se formuló el borrador del DRP sin ejecución completa ni aprobación formal. En 2026 se implementa bajo gobernanza institucional, con pruebas trimestrales y simulaciones anuales, asegurando cumplimiento normativo y defendibilidad ante auditoría.

La transición 2025 → 2026 obedece a la maduración natural del ciclo PHVA del SGSI: el diagnóstico realizado en 2025 se convierte en 2026 en operación formal del DRP, alineada con las cláusulas 8 y 9.1 de **ISO/IEC 27001:2022** y con el control 5.30 de **ISO/IEC 27002:2022**. Las pruebas, métricas e informes quedan versionados en el repositorio SGSI conforme al control 5.3.

Gestión y evidencias

Las pruebas, métricas, evidencias y ajustes del DRP se administran en el documento específico, controlado en el repositorio oficial del SGSI y sujeto a revisión periódica por el Mesa de Trabajo SGSI. El PTRSPI mantiene la trazabilidad mediante indicadores estratégicos, tales como:

- **% pruebas de restauración exitosas**

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

- **MTTR (Mean Time to Recovery)**
- **MTTD (Mean Time to Detect)**

La fuente de datos para estos indicadores son los informes del DRP aprobados en comité.

8.4.1. Relación normativa y contractual

Esta referencia asegura el cumplimiento de:

- Requisitos de **continuidad del negocio**
- **Defendibilidad ante auditorías**
- Obligaciones contractuales en materia de **resiliencia tecnológica.**

8.4.2. Control documental

Todas las pruebas, métricas y evidencias del DRP se registran y versionan en:

- **riesgos del PTRSPI**
- **Repositorio SGSI**

8.5. Plan de verificación y mejora continua (PHVA)

Propósito

Garantizar la mejora continua del PTRSPI mediante la operación del ciclo **PHVA (Planear–Hacer–Verificar–**

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Actuar), integrando la **evaluación de madurez** y el **apetito/tolerancia/capacidad de riesgo** (Guía v7) como insumos para priorización y decisiones estratégicas, y articulando **KRI/KPI** con las **líneas de aseguramiento (MECI)** para sostener defendibilidad ante auditoría interna y externa del **SGSI**.

8.5.1. Gobernanza y tono desde la cima

La **Alta Dirección** sostiene el "**tono desde la cima**" y supervisa la aceptación, transferencia y evitación de riesgos, aprobando los umbrales del **apetito** institucional y las acciones correctivas, con evidencia en **actas de comité** y **control de versiones** del **SGSI**, conforme a **ISO/IEC 27001:2022 cl. 6.1.3** y al ciclo **PHVA**.

Fase PHVA	Actividades clave (ajustadas)	Responsable	Frecuencia	Evidencia esperada
Planificar (P)	Definir objetivos, KPI y KRI; actualizar apetito/tolerancia/capacidad de riesgo; evaluar madurez (Guía v7); programar auditorías internas y externas; validar en Mesa de Trabajo SGSI	Dirección TIC, Mesa de Trabajo SGSI (cuando exista) o CIGD	Anual	Acta Mesa de Trabajo SGSI; plan de auditoría; matriz de madurez/apetito
Hacer (H)	Ejecutar actividades del PTRSPI (continuidad, MFA, vulnerabilidades, baseline cloud, cifrado); registrar evidencias en repositorio SGSI	Propietarios de proceso, Seguridad TI	Continuo	Informes de ejecución; SOA actualizada; checklist línea base cloud; Registro

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Fase PHVA	Actividades clave (ajustadas)	Responsable	Frecuencia	Evidencia esperada
	con control documental (ISO 27001, 5.3); Actualizar mapa institucional con riesgos críticos del PTRSPI			actualizado del mapa institucional con folio 5.3
Verificar (V)	Revisar KPI y KRI; auditar desempeño SGSI; validar cumplimiento ISO 27001 cl. 9.1 y 9.2; reporte en líneas de aseguramiento (MECI); evaluar resultados de pruebas DRP y controles críticos	Control Interno, Auditoría	Trimestral / Semestral	Informes de auditoría; KPIs/KRIs validados; actas de comité
Actuar (A)	Incorporar hallazgos; ajustar controles y recursos; aprobar cambios del PTRSPI por Alta Dirección (Tone at the Top); publicar actualización en repositorio SGSI con control de versiones	Alta Dirección, Comité Institucional	Anual	Acta de actualización del PTRSPI; registro de decisiones de aceptación/transferencia

Tabla 14 – PHVA

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

8.5.2. Mapa de calor de riesgos críticos

El **mapa de calor** presenta, de forma visual, los **riesgos priorizados** del PTRSPI clasificados como **Altos y Extremos**, indicando su **nivel de criticidad** (calculado con la fórmula *Impacto × Probabilidad*), el **estado de tratamiento** según el **Informe GAP** y los **controles aplicados** conforme a **ISO/IEC 27002:2022**.

La información se obtiene de la **matriz integrada de trazabilidad del riesgo** y del **Informe GAP**, evitando duplicidad con el **Mapa de Riesgos Institucional**. Este recurso tiene como objetivo:

- Garantizar la **defendibilidad ante auditoría**
- Mantener la **trazabilidad con los KPIs del PTRSPI** y los registros en el **repositorio SGSI** bajo control documental (**ISO/IEC 27001:2022, control 5.3**)

ID riesgo	Descripción breve	Nivel (1–25)	Clasificación	Control ISO/IEC 27002	Estado (GAP)	KPI (Desempeño)	Meta	KRI (Preventivo)	Umbral alerta	Frecuencia de medición	Evidencia
R01	Indisponibilidad de servicios críticos	20	Extremo	5.30 Continuidad	Parcial	% pruebas restauración exitosas	≥90 %	% servicios críticos sin prueba DRP en trimestre	>10 %	Trimestral	Acta Mesa de Trabajo SGSI (cuando exista) o

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ID riesgo	Descripción breve	Nivel (1–25)	Clasificación	Control ISO/IEC 27002	Estado (GAP)	KPI (Desempeño)	Meta	KRI (Preventivo)	Umbral alerta	Frecuencia de medición	Evidencia
											CIGD + Informe DRP
R02	Compromiso de cuentas de correo	12	Alto	8.2 Control de acceso	Parcial	% cuentas con MFA	≥90 %	% cuentas sin MFA habilitado	>5%	Mensual	Reporte plataforma MFA
R03	Vulnerabilidades críticas en web	15	Alto	8.8 Gestión de vulnerabilidades	Parcial	% vulns corregidas en SLA	≥95 %	% vulns fuera de SLA	>10 %	Mensual	Informes de escaneo / tickets
R04	Configuración insegura en nube	14	Alto	5.23 Seguridad en nube	Parcial	% cumplimiento línea base cloud	≥90 %	% controles cloud sin aplicar	>15 %	Trimestral	Checklist línea base cloud

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

ID riesgo	Descripción breve	Nivel (1–25)	Clasificación	Control ISO/IEC 27002	Estado (GAP)	KPI (Desempeño)	Meta	KRI (Preventivo)	Umbral alerta	Frecuencia de medición	Evidencia
R05	Datos sin cifrado	16	Extremo	8.24 Criptografía	No iniciado/Parcial	% cifrado en tránsito y reposo	≥95 %	% repositorios sin cifrado	>10 %	Trimestral	Informe de cifrado / backup
R06	Vulns en cargas cloud	12	Alto	8.8 Gestión de vulnerabilidades	Parcial	% vulns corregidas en SLA	≥95 %	% vulns fuera de SLA	>10 %	Mensual	Informe escaneo cloud
R07	Indisponibilidad SaaS por proveedor	13	Alto	5.30 + 5.19 Acuerdos externos	Parcial	% pruebas continuidad SaaS	≥90 %	% ANS sin validación trimestral	>10 %	Trimestral	Actas pruebas + ANS proveedor

Ilustración 1 - Mapa de calor

8.5.3. Flujo de retroalimentación

El flujo de retroalimentación asegura la integración sistemática de hallazgos y resultados en la mejora continua del PTRSPI. Cada ciclo inicia con la recopilación de evidencias provenientes de auditorías, revisiones de KPIs y análisis del Informe GAP, las cuales son evaluadas en el Mesa de Trabajo SGSI. Posteriormente, se definen ajustes y acciones correctivas que son validadas por el Comité Institucional,

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

garantizando su aprobación formal. Finalmente, las actualizaciones se publican en el repositorio SGSI, cerrando el ciclo y asegurando trazabilidad, defendibilidad ante auditoría y alineación con el ciclo PHVA conforme a ISO / IEC 27001:2022 y lineamientos MinTIC.

Ilustración 2 - Flujo de retroalimentación

8.5.4. Referencia normativa

Este apartado se fundamenta en los requisitos establecidos por **ISO / IEC 27001:2022**, específicamente en las cláusulas 9.1 (Seguimiento, medición, análisis y evaluación), 9.2 (Auditoría interna) y 10.2 (Acciones correctivas), así como en los lineamientos del Modelo de Seguridad y Privacidad de la Información – MinTIC (LI.ES.06). Estas referencias garantizan la trazabilidad, la mejora continua y la conformidad del PTRSPI con estándares internacionales y regulaciones nacionales.

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

9. Trazabilidad del riesgo

La matriz de trazabilidad se encuentra en el *Mapa de Riesgos Institucional* de la Empresa de Renovación y Desarrollo Urbano de Bogotá, D.C., conforme a la metodología DAFP versión 6 (nov. 2022), donde se documentan: identificación, valoración, priorización, controles asociados y evidencias.

El Plan de Tratamiento de Riesgos **no duplica la matriz**, sino que **actúa sobre los riesgos priorizados** (Altos y Extremos), conforme a la Resolución MinTIC 500 de 2021, que obliga a articular la gestión de riesgos de seguridad digital al sistema institucional y reportarla al Comité Institucional.

Para cada riesgo priorizado, el plan establece:

- Actividad de tratamiento
- Control ISO 27001:2022 (Anexo A)
- Responsable
- Evidencia requerida
- Fecha de inicio y fin

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ID Riesgo	Descripción	Activo/Proceso	Nivel	Control ISO	Actividad	KPI	Meta	Evidencia	Responsable	Plazo	PETI/PSPI	Contrato
R-01	Indisponibilidad de servicios críticos	Infraestructura TI	Extremo	5.30 Continuidad	Validar evidencias del DRP en Mesa de Trabajo SGSI (ver Anexo 2 o DRP en repositorio SGSI).	% pruebas restauración exitosas	≥ 90%	Acta Mesa de Trabajo SGSI + Informe DRP (repositorio SGSI).	Infraestructura	Q2/2026	OE-TI 3 / KPI Continuidad	Cl. Quinta (Continuidad)
R-02	Compromiso de cuentas de correo	Correo institucional	Alto	8.2 Control de acceso	Activar MFA en cuentas	% cuentas con MFA	≥90%	Reporte plataforma	Gestión TIC	Q2/2026	OE-TI 3 / KPI MFA	Cl. Vigésima Octava (Confidencialidad)
R-03	Vulnerabilidades críticas en web	Portal Web	Alto	8.8 Gestión de vulnerabilidades	Escaneo y remediación mensual	% vulnerabilidades corregidas en SLA	≥95%	Informe escaneo	Seguridad	Mensual	OE-TI 3 / KPI Vulnerabilidades	Cl. Quinta (Seguridad digital)

ID Riesgo	Descripción	Activo/Proceso	Nivel	Control ISO	Actividad	KPI	Meta	Evidencia	Responsable	Plazo	PETI/PSPI	Contrato
R-04	Configuración insegura de servicios en la nube (permisos excesivos, exposición pública)	Nube pública/privada (Google Workspace, SaaS críticos)	Alto	5.23 Seguridad en servicios en la nube	Definir y aplicar línea base de seguridad en nube	Definir y aplicar línea base de seguridad cloud (hardening, logging, segmentación)	% cumplimiento línea base cloud	≥ 90%	Checklist línea base cloud; reportes de configuración	Seguridad de la Información	Q2/2026	OE-TI 3 / PSPI KPI Seguridad cloud
R-05	Datos en la nube sin cifrado en tránsito o en reposo	Nube (repositorios, backups, bases de datos SaaS)	Alto	8.24 Criptografía (política de cifrado)	Implementar cifrado TLS en tránsito y cifrado en reposo	Implementar cifrado TLS en tránsito y cifrado en reposo (DB/backup)	% cifrado en tránsito y reposo	≥ 95%	Informes de configuración TLS /	Seguridad de la Información	Q2/2026	OE-TI 3 / PETI KPI Cifrado
R-06	Vulnerabilidades técnicas en cargas de trabajo en la nube (VM / contenedores)	Nube privada (servicios críticos) / cargas IaaS	Alto	8.8 Gestión de vulnerabilidades	Escaneo y remediación de vulnerabilidades en cargas cloud	Escaneo programado y remediación con SLAs en ambientes cloud	% vulnerabilidades corregidas en SLA	≥ 95%	Informes de escaneo cloud; tickets de	Seguridad	Mensual	OE-TI 3 / PSPI KPI Vulnerabilidades
R-07	Indisponibilidad de servicios SaaS críticos por fallas del proveedor	Servicios SaaS (ERP JSP7, SGDEA TAMPUS, correo)	Alto	5.30 Continuidad; 5.19 Acuerdos con partes externas	Revisión y fortalecimiento de ANS con proveedores críticos (SaaS/ERP/SGDEA)	Plan de continuidad específico para SaaS (RTO / RPO, salidas de emergencia)	% pruebas de restauración/continuidad SaaS exitosas	≥ 90%	Actas de pruebas y acuerdos ANS con proveedores	Infraestructura / Gestión de Proveedores	Trimestral	OE-TI 3 / PSPI KPI Continuidad

Tabla 15 - Matriz integrada de trazabilidad del riesgo

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

10. Indicadores de desempeño

Los indicadores definidos en el PTRSPI son instrumentos estratégicos para la toma de decisiones del Mesa de Trabajo SGSI y del Comité Institucional, no simples elementos informativos. Su análisis periódico permite ajustar prioridades, reasignar recursos y redefinir estrategias de tratamiento del riesgo cuando sea necesario.

Se diferencian los KPI (indicadores de desempeño) y los KRI (indicadores clave de riesgo) conforme a la Guía v7 (2025), incorporando frecuencia de medición y umbrales preventivos para activar acciones correctivas en el ciclo PHVA y reporte en líneas de aseguramiento (MECI).

La siguiente tabla consolida los indicadores establecidos en el PTRSPI, incluyendo:

- Indicador
- Tipo (KPI/KRI)
- Meta o Umbral
- Fórmula de cálculo
- Línea base inicial
- Fuente de datos

- Periodicidad
- Responsable
- Relación normativa

Acción correctiva

Esta estructura garantiza trazabilidad, reproducibilidad y mejora continua, en conformidad con ISO/IEC 27001:2022 y la Guía v7. Las evidencias y cálculos detallados se consolidan en el Anexo 2: Matriz de trazabilidad de riesgos, que actúa como repositorio auditable para sostener la defendibilidad ante auditoría.

Indicador	Tipo	Meta / Umbral	Fórmula de cálculo	Línea base inicial	Fuente de datos	Periodicidad	Responsable	Relación normativa	Acción correctiva
% riesgos críticos mitigados	KPI	Meta ≥90% / Umbral <80%	(Riesgos críticos mitigados / Total riesgos críticos identificados) × 100	45% (Informe GAP 2025)	Matriz SGSI / Informe GAP	Trimestral	Seguridad de la Información	ISO 27001 cl. 6.1.3; MinTIC LI.GS.02	Activar plan de contingencia, revisión en Mesa de Trabajo SGSI

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Tipo	Meta / Umbral	Fórmula de cálculo	Línea base inicial	Fuente de datos	Periodicidad	Responsable	Relación normativa	Acción correctiva
									(cuando exista) o CIGD
% controles ISO implementados	KPI	Meta ≥90% / Umbral <75%	(Controles implementados / Total controles aplicables) × 100	52%	SOA / Auditoría interna	Trimestral	Dirección TIC	ISO 27001 cl. 8.1; ISO 27002 5–8	Revisión SOA, asignar responsable
% activos clasificados	KPI	Meta ≥95% / Umbral <80%	(Activos clasificados / Total activos inventariados) × 100	60%	Inventario de activos	Semestral	Dirección TIC	ISO 27002 5.9	Campaña de actualización
Nivel de madurez MSPI	KPI	Meta ≥4 / Umbral <3	Valor obtenido según metodología Guía v7	Nivel 3	Evaluación MSPI	Anual	Planeación / TIC	Guía v7; MinTIC LI.UA.03	Implementar plan de formación
MTTD incidentes	KPI	Meta ≤48h /	Σ tiempo detección / Nº incidentes	72h	Registros CSIRT	Mensual	Seguridad	ISO 27002 5.24	Optimizar monitoreo

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Tipo	Meta / Umbral	Fórmula de cálculo	Línea base inicial	Fuente de datos	Periodicidad	Responsable	Relación normativa	Acción correctiva
		Umbral >72h							
MTTR incidentes	KPI	Meta ≤72h / Umbral >96h	Σ tiempo resolución / Nº incidentes	96h	Registros CSIRT	Mensual	Seguridad	ISO 27002 5.24	Reforzar protocolos
% pruebas DRP exitosas	KPI	Meta ≥90% / Umbral <70%	(Pruebas exitosas / Total pruebas) × 100	70%	Informes DRP	Trimestral	Infraestructura	ISO 27001 cl. 8.4; MinTIC LI.ST.04	Actualizar DRP
% cuentas con MFA	KPI	Meta ≥90% / Umbral <75%	(Cuentas con MFA / Total cuentas) × 100	62%	Reporte MFA	Mensual	Gestión TIC	ISO 27002 8.2	Campaña activación MFA
% vulnerabilidades corregidas en SLA	KPI	Meta ≥95% /	(Vulns corregidas en SLA / Total vulns) × 100	54%	Informes escaneo	Mensual	Seguridad	ISO 27002 8.8	Ajustar ciclo escaneo

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Tipo	Meta / Umbral	Fórmula de cálculo	Línea base inicial	Fuente de datos	Periodicidad	Responsable	Relación normativa	Acción correctiva
		Umbral <80%							
% cumplimiento línea base cloud	KPI	Meta ≥90% / Umbral <70%	(Controles aplicados / Total definidos) × 100	50%	Checklist cloud	Trimestral	Seguridad de la Información	ISO 27002 5.23	Aplicar controles faltantes
% cifrado en tránsito y reposo	KPI	Meta ≥95% / Umbral <80%	(Servicios cifrados / Total servicios críticos) × 100	40%	Informes TLS/cifrado	Trimestral	Seguridad de la Información	ISO 27002 8.24	Implementar cifrado
% PIAs ejecutadas	KPI	Meta ≥90% / Umbral <70%	(PIAs completadas / Total PIAs requeridas) × 100	30%	Registros SGSI	Semestral	Seguridad / Jurídica	ISO 27002 5.34	Agendar PIAs pendientes
% hallazgos cerrados	KPI	Meta ≥90% /	(Hallazgos cerrados / Total hallazgos) × 100	65%	Informes auditoría	Trimestral	Control Interno	ISO 27001 cl. 9.1, 10.2;	Activar plan de mejora

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Tipo	Meta / Umbral	Fórmula de cálculo	Línea base inicial	Fuente de datos	Periodicidad	Responsable	Relación normativa	Acción correctiva
		Umbral <80%						MinTIC LI.ES.06	
% riesgos críticos del PTRSPI incorporados al mapa institucional	KPI	100% / <100%	(Riesgos críticos del PTRSPI registrados en el mapa institucional / Total riesgos críticos del PTRSPI) × 100	Ciclo 2025, actividad no ejecutada	Matriz institucional de riesgos + actas y repositorio SGSI.	Trimestral	Gestión TIC / Seguridad	ISO/IEC 27001:2022 cl. 6.1.3; control 5.3; Guía DAFP v7	Escalamiento a Mesa de Trabajo SGSI (cuando exista) o CIGD.
% vulns fuera de SLA	KRI	Umbral >10%	(Vulns fuera de SLA / Total vulns) × 100	—	Informes escaneo	Mensual	Seguridad	ISO 27002 8.8; Guía v7	Escalamiento a Mesa de Trabajo SGSI (cuando exista) o CIGD.
% cuentas sin MFA	KRI	Umbral >5%	(Cuentas sin MFA / Total cuentas) × 100	—	Reporte MFA	Mensual	Gestión TIC	ISO 27002 8.2; Guía v7	Bloqueo temporal

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Tipo	Meta / Umbral	Fórmula de cálculo	Línea base inicial	Fuente de datos	Periodicidad	Responsable	Relación normativa	Acción correctiva
% servicios críticos sin prueba DRP	KRI	Umbral >10%	(Servicios sin prueba / Total servicios críticos) × 100	—	Informes DRP	Trimestral	Infraestructura	ISO 27002 5.30; Guía v7	Activar pruebas
% incumplimiento WCAG 2.1 AA	KRI	Umbral >5%	(Portales no conformes / Portales críticos) × 100	—	Informes validación AA	Trimestral	Dirección TIC	Circular 007/2024; ISO 27001 5.3	Plan de adecuación

Tabla 16 – KPI y KRI

Además de los **KPI (Key Performance Indicators)** definidos para medir el desempeño operativo del PTRSPI, se incorporan **KRI (Key Risk Indicators)** como instrumentos de monitoreo preventivo, en cumplimiento de la **Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 (2025)**.

Los **KRI** permiten anticipar la materialización de riesgos críticos (continuidad, accesos, vulnerabilidades, cifrado, accesibilidad digital) y se diferencian de los KPI porque se enfocan en señales tempranas y umbrales de alerta.

Su reporte se articula con las **líneas de aseguramiento (MECI)** y el ciclo **PHVA**, garantizando trazabilidad y defendibilidad ante auditoría.

Ejemplos de KRI:

- **% vulnerabilidades detectadas fuera de SLA**

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

- **% cuentas sin MFA habilitado**
- **% incumplimiento WCAG 2.1 AA en portales críticos**
- **% servicios críticos sin pruebas DRP en el trimestre**

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

11. Conclusiones

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información constituye un instrumento clave para la gestión integral del riesgo institucional. Su correcta implementación requiere no solo el despliegue de controles técnicos, sino el compromiso de la Alta Dirección y de los procesos en la toma de decisiones informadas frente al riesgo, garantizando la continuidad del negocio, el cumplimiento normativo y la protección de la información de la Entidad.

12. Anexos

12.1. Anexo 1: Integración del mapa de riesgos del SGSI, cronograma DRP y línea base de indicadores

12.1.1. Contexto y propósito

Este anexo consolida, para efectos del Sistema de Gestión de Seguridad de la Información (SGSI), la integración del mapa de riesgos del SGSI, la referencia al Plan de Recuperación Tecnológica ante Desastres (DRP) y la definición de la línea base de indicadores. El objetivo es asegurar trazabilidad normativa y defendibilidad ante auditoría externa conforme a **ISO / IEC 27001:2022** y al Modelo MinTIC, en coherencia con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI).

12.1.2. Integración del mapa de riesgo del SGSI

La matriz resume los riesgos críticos identificados en la fase 1 (identificación de activos y riesgos), con vinculación a controles ISO/IEC 27001:2022, propietario y fecha objetivo. La fuente de verdad dinámica permanece en el archivo institucional ‘Inventario_Activos_RenoBo.xlsx’.

El mapa integra **indicadores de desempeño (KPI)** e **indicadores clave de riesgo (KRI)** con **metas/umbrales**, **frecuencia de medición** y **evidencia**, alineados con **ISO/IEC 27001:2022** (seguimiento y auditoría), **ISO/IEC 27002:2022** (controles 5.30, 8.2, 8.8, 5.23, 8.24) y reporte en **líneas de aseguramiento (MECI)**, conforme a la **Guía v7 (2025)**.

ID riesgo	Descripción breve	Nivel (1–25)	Clasificación	Control ISO/IEC 27002	Estado (GAP)	KPI (Desempeño)	Meta	KRI (Preventivo)	Umbral alerta	Frecuencia	Evidencia
R01	Indisponibilidad de servicios críticos	20	Extremo	5.30 Continuidad	Parcial	% pruebas DRP exitosas	≥90%	% servicios críticos sin prueba DRP	>10%	Trimestral	Acta Mesa de Trabajo SGSI (cuando exista) o CIGD + Informe DRP
R02	Compromiso de cuentas de correo	12	Alto	8.2 Control de acceso	Parcial	% cuentas con MFA	≥90%	% cuentas sin MFA	>5%	Mensual	Reporte plataforma MFA

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

ID riesgo	Descripción breve	Nivel (1–25)	Clasificación	Control ISO/IEC 27002	Estado (GAP)	KPI (Desempeño)	Meta	KRI (Preventivo)	Umbral alerta	Frecuencia	Evidencia
R03	Vulnerabilidades críticas en web	15	Alto	8.8 Gestión de vulnerabilidades	Parcial	% vulns corregidas en SLA	≥95%	% vulns fuera de SLA	>10%	Mensual	Escaneos + tickets
R04	Configuración insegura en nube	14	Alto	5.23 Seguridad en nube	Parcial	% cumplimiento línea base cloud	≥90%	% controles cloud sin aplicar	>15%	Trimestral	Checklist línea base cloud
R05	Datos sin cifrado	16	Extremo	8.24 Criptografía	No iniciado/Parcial	% cifrado en tránsito y reposo	≥95%	% repositorios sin cifrado	>10%	Trimestral	Informe de cifrado / backup

Tabla 17 - Extracto con activos críticos

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

12.1.3. Cronograma de pruebas del DRP

El cronograma consolida pruebas planificadas del DRP con sus objetivos, responsables y evidencias esperadas, y se articula con los objetivos de RTO y RPO definidos para servicios críticos.

Prueba	Objetivo	Fecha estimada	Evidencia esperada	Responsable
Prueba 1: Restauración de ERP JSP7	Validar RTO ≤8h y RPO ≤4h	Febrero 2026	Informe de restauración, bitácora de tiempos, acta Mesa de Trabajo SGSI (cuando exista) o CIGD	Infraestructura TI
Prueba 2: Recuperación correo institucional	Validar continuidad SaaS crítico	Abril 2026	Reporte de recuperación, checklist ANS proveedor	Gestión TIC
Prueba 3: Simulación de ataque ransomware	Evaluar respuesta ante incidente crítico	Junio 2026	Informe análisis forense, registro de notificación CSIRT	Seguridad de la Información
Prueba 4: Restauración SGDEA TAMPUS	Validar integridad documental	Julio 2026	Evidencia restauración, acta validación	Infraestructura TI

Prueba	Objetivo	Fecha estimada	Evidencia esperada	Responsable
Prueba 5: Prueba integral DRP	Validar coordinación interprocesos	Agosto 2026	Acta Mesa de Trabajo SGSI (cuando exista) o CIGD, informe consolidado	Dirección TIC

Tabla 18 - Cronograma de pruebas

12.1.4. Línea base de indicadores del PTRSPI

La línea base constituye el punto de partida para la verificación trimestral y la mejora continua (PHVA). Los valores se consolidan de informes y matrices institucionales del SGSI.

Indicador	Línea base	Meta / Umbral	Periodicidad	Fuente
% activos clasificados	60%	Meta ≥95% / Umbral <80%	Semestral	Inventario de activos / Mesa de Trabajo SGSI (cuando exista) o CIGD
% riesgos críticos mitigados	45%	Meta ≥90% / Umbral <80%	Trimestral	Matriz SGSI / Informe GAP

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Línea base	Meta / Umbral	Periodicidad	Fuente
% controles ISO implementados	52%	Meta ≥90% / Umbral <75%	Trimestral	SOA / Auditoría interna
% pruebas DRP exitosas	70%	Meta ≥90% / Umbral <70%	Trimestral	Informes DRP / Actas Mesa de Trabajo SGSI (cuando exista) o CIGD
% cuentas con MFA	62%	Meta ≥90% / Umbral <75%	Mensual	Reporte plataforma MFA
% cifrado en tránsito y reposo	40%	Meta ≥95% / Umbral <80%	Trimestral	Informes configuración TLS / cifrado
% vulnerabilidades corregidas en SLA	54%	Meta ≥95% / Umbral <80%	Mensual	Informes escaneo / tickets
% cumplimiento línea base cloud	50%	Meta ≥90% / Umbral <70%	Trimestral	Checklist seguridad cloud
Nivel de madurez MSPI (Guía v7)	Nivel 3	Meta ≥4 / Umbral <3	Anual	Evaluación MSPI / Autoevaluación (Cap. 10)

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Indicador	Línea base	Meta / Umbral	Periodicidad	Fuente
% PIAs ejecutadas	30%	Meta ≥90% / Umbral <70%	Semestral	Registros SGSI / Mesa de Trabajo SGSI (cuando exista) o CIGD
% reducción del riesgo residual vs inicial	N/D	—	Trimestral (primer corte)	Matriz de riesgos (primer corte trimestral)

Tabla 19 - Línea base de indicadores

12.1.5. Plantilla para seguimiento de KPI y KRI

Plantilla para registrar resultados, metas (KPI) y umbrales (KRI), frecuencia y acciones correctivas conforme a **ISO/IEC 27001:2022** y **Guía v7 (Cap. VIII)** (reporte en líneas de aseguramiento – MECI).

Indicador	Tipo	Fórmula	Fuente	Línea base	Meta / Umbral	Periodicidad	Responsable
% activos clasificados	KPI	(Activos clasificados /	Inventario de activos	60%	Meta ≥95% /	Semestral	Dirección TIC

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Indicador	Tipo	Fórmula	Fuente	Línea base	Meta / Umbral	Periodicidad	Responsable
		Total inventariados) × 100			Umbral <80%		
% riesgos críticos mitigados	KPI	(Riesgos mitigados / Riesgos críticos) × 100	Matriz SGSI	45%	Meta ≥90% / Umbral <80%	Trimestral	Seguridad de la Información
% pruebas DRP exitosas	KPI	(Pruebas exitosas / Total pruebas) × 100	Informes DRP	70%	Meta ≥90% / Umbral <70%	Trimestral	Infraestructura TI
% cuentas con MFA	KPI	(Cuentas con MFA / Cuentas activas) × 100	Reporte MFA	62%	Meta ≥90% /	Mensual	Gestión TIC

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Tipo	Fórmula	Fuente	Línea base	Meta / Umbral	Periodicidad	Responsable
					Umbral <75%		
% cifrado en tránsito y reposo	KPI	(Servicios cifrados / Servicios críticos) × 100	Informes TLS/cifrado	40%	Meta ≥95% / Umbral <80%	Trimestral	Seguridad de la Información
% vulns fuera de SLA	KRI	(Vulns fuera de SLA / Total vulns) × 100	Informes escaneo/tickets	--	Umbral >10%	Mensual	Seguridad
% cuentas sin MFA	KRI	(Cuentas sin MFA / Total cuentas) × 100	Reporte MFA	--	Umbral >5%	Mensual	Gestión TIC

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Indicador	Tipo	Fórmula	Fuente	Línea base	Meta / Umbral	Periodicidad	Responsable
% servicios críticos sin prueba DRP	KRI	(Servicios sin prueba / Total servicios críticos) × 100	Informes DRP	--	Umbral >10%	Trimestral	Infraestructura

Tabla 20 - Plantilla de seguimiento de ***KPIs***

12.1.6. Gobernanza y evidencias

Gobernanza del SGSI y "tono desde la cima"

La toma de decisiones sobre tratamiento del riesgo (aceptar, mitigar, transferir o evitar) se rige por la gobernanza institucional del **SGSI**, con aprobación por **Alta Dirección** y registro en actas, sustentada en el control documental **5.3** de **ISO/IEC 27001:2022**. Este principio asegura el "**tono desde la cima**" y la defendibilidad ante auditoría, en concordancia con el ciclo **PHVA** y la estructura de comités definida en el PTRSPI 2026–2029.

Roles y responsabilidades

Se mantienen los roles y responsabilidades institucionales para la gestión de riesgos de seguridad y privacidad de la información, con trazabilidad a propietarios de activos/riesgos, responsables de implementación y órganos de control, de acuerdo con la matriz de roles y la RACI del documento base.

Flujo de escalamiento

El escalamiento para **riesgos no mitigados e incidentes críticos** opera conforme a los niveles y tiempos establecidos, garantizando oportunidad de respuesta y registro en comités:

- Nivel 1: Responsable del proceso → Hasta su creación, la revisión se realiza en el Mesa de Trabajo SGSI (cuando exista) o CIGD. (máx. 24 horas)
- **Nivel 2:** Dirección Administrativa y TIC → **Alta Dirección** (máx. 48 horas)
- **Nivel 3:** Alta Dirección → **Comité Institucional** (máx. 72 horas)

  Las actuaciones se evidencian en **actas** y **registros** de la **Matriz de trazabilidad** (Anexo 2).

Criterios y aprobaciones

La **aceptación** de riesgos altos y extremos, así como la **transferencia/evitación** de riesgos residuales, corresponde **exclusivamente a la Alta Dirección** y debe constar en actas del **Comité Institucional**, con soporte en **ISO/IEC 27001:2022 cl. 6.1.3** y control de versiones del SGSI (5.3).

Control documental y repositorio SGSI

Todas las evidencias y decisiones se **versionan** y **publican** en el **repositorio oficial del SGSI** como **fuente única de verdad**, siguiendo el control **5.3** de **ISO/IEC 27001:2022**. Esto incluye políticas, **SOA**, anexos, cronogramas, informes y actas de comité, asegurando trazabilidad, reproducibilidad y defendibilidad ante auditorías internas y externas.

Líneas de aseguramiento (MECI) y PHVA

- Planear (P): definición de objetivos, KPI y KRI, actualización de apetito/tolerancia y programación de auditorías; validación en Mesa de Trabajo SGSI.
- **Hacer (H):** ejecución de actividades priorizadas (continuidad/DRP, MFA, vulnerabilidades, baseline cloud, cifrado) y registro de evidencias en el repositorio SGSI con control 5.3.
- **Verificar (V):** revisión de **KPI/KRI**, evaluación de desempeño del SGSI y resultados de pruebas, con reporte en líneas de aseguramiento (Control Interno/Auditoría) y actas de comité.
- **Actuar (A):** incorporación de hallazgos, ajustes y **aprobación por Alta Dirección**; publicación de actualizaciones con control de versiones (5.3).

Evidencias mínimas

Para sustentar la operación y el seguimiento del PTRSPI se deberá contar, como mínimo, con:

- Actas de Mesa de Trabajo SGSI y Comité Institucional (decisiones, aceptaciones/transferencias, umbrales y acciones correctivas).

- **Informes DRP** (pruebas de restauración, RTO/RPO, resultados por servicio crítico).
- **Reportes MFA** (cobertura y cuentas con/sin MFA, acciones de bloqueo o activación).
- **Informes de escaneo y tickets de remediación** (cumplimiento de **SLA** en vulnerabilidades).
- **Checklist y auditorías de configuración cloud** (cumplimiento de baseline/hardening).
- **Informes de cifrado** en tránsito y reposo (TLS, BD/backup) con auditoría correspondiente.
- **Validaciones de accesibilidad WCAG 2.1 AA** y actas de aprobación (cuando aplique por Circular 007/2024).

Relación con partes externas y contratos

Para **proveedores críticos** (ERP, nube, SaaS) se exigirán **cláusulas de continuidad y seguridad digital**, así como la verificación de **ANS** compatibles con el **DRP**. Las pólizas y acuerdos de transferencia de riesgos se registran como evidencia en el repositorio SGSI y en la **Matriz de trazabilidad** (Anexo 2).

12.1.7. Referencias normativas y contractuales

- ISO/IEC 27001:2022 (cláusulas 6.1.2, 6.1.3, 8.4, 9.1, 9.2, 10.2)
- **ISO / IEC 27002:2022** (controles 5.19, 5.23, 5.30, 8.2, 8.7, 8.8, 8.12, 8.20, 8.22, 8.23, 8.24)

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

- Modelo de Seguridad y Privacidad de la Información — MinTIC (Resolución 500/2021; Decreto 767/2022).

12.1.8. Matriz de madurez y apetito/tolerancia/capacidad (Guía v7)

Objetivo

Incorporar la **evaluación de madurez** y el **apetito/tolerancia/capacidad de riesgo** como insumos metodológicos para priorización de brechas y decisiones estratégicas (Guía v7).

Componente (COSO-ERM)	Principios clave	Evidencia existente	Nivel (1–5)	Brecha identificada	Acción propuesta	Plazo	Responsable	Acta/Folio (Gobernanza 5.3)
Gobernanza y cultura	"Tono desde la cima", roles y responsabilidades, comités	Actas Mesa de Trabajo SGSI/Institucional; Matriz RACI	3	Política de apetito no formalizada	Aprobar política de apetito y tolerancia en Comité Institucional	Q2/2026	Dirección TIC / Alta Dirección	Acta CI-##/2026; Folio SGSI V5.3

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Componente (COSO-ERM)	Principios clave	Evidencia existente	Nivel (1–5)	Brecha identificada	Acción propuesta	Plazo	Responsable	Acta/Folio (Gobernanza 5.3)
Estrategia y objetivos	Alineación PTRSPI–PETI–PSPI; criterios de aceptación	Vinculación EO0203; criterios de aceptación (Tabla 11)	3	Falta trazar metas de riesgo por objetivo OE-TI	Integrar metas/KPI de riesgo por OE-TI en Cap. 8 y Anexos	Q2/2026	Planeación / TIC	Acta SGSI-##/2026; actualización SOA
Desempeño	Identificación y priorización; KRI/KPI operando	Tabla 16; Mapa de calor con KRI/KPI y frecuencia	2	Umbrales KRI incompletos	Definir/aprobar umbrales KRI y frecuencias (MECI)	Q1/2026	Seguridad / Control Interno	Acta SGSI-##/2026; repositorio SGSI 5.3
Revisión y monitoreo	PHVA; auditoría interna; seguimiento GAP	Tabla PHVA; informes auditoría; GAP ISO/MSPI	3	Faltan cortes trimestrales consolidados	Calendarizar cortes y publicar informes con	Q1–Q4/2026	Control Interno / Auditoría	Acta Auditoría-##/2026; folio 5.3

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Componente (COSO-ERM)	Principios clave	Evidencia existente	Nivel (1–5)	Brecha identificada	Acción propuesta	Plazo	Responsable	Acta/Folio (Gobernanza 5.3)
					control de versión			
Información, comunicación y reporte	Repositorio SGSI; control 5.3; evidencias	Políticas/SOA/Anexos versionados	4	Estructura de metadatos no homogénea	Normalizar metadatos (indicador, fecha, versión, comité)	Q1/2026	SGSI / Archivo	Registro SGSI; control 5.3

Tabla 21 - Matriz de madurez y apetito/tolerancia/capacidad

12.2. Anexo 2: Matriz de trazabilidad de riesgos

ID Riesgo	Actividad	ISO 27001	ISO 27002	KPI	Meta	Brecha ISO/MSPI cerrada	Responsable
R-01	Implementar redundancia en servidores críticos	8.1	8.1	% disponibilidad de servicios críticos	>=99.9%	GAP: Cláusula 8.1 – Gestión de activos (Estado inicial: Parcial)	Área Infraestructura TI
R-02	Fortalecer autenticación multifactor en correo institucional	9.4	9.4	% cuentas con MFA habilitado	>=95%	GAP: Cláusula 9.4 – Control de acceso (Estado inicial: No iniciado)	Área Seguridad TI
R-03	Aplicar parches críticos en portal web	8.8	8.8	% vulnerabilidades críticas corregidas	>=100%	GAP: Cláusula 8.8 – Gestión de vulnerabilidades	Área Desarrollo

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

ID Riesgo	Actividad	ISO 27001	ISO 27002	KPI	Meta	Brecha ISO/MSPI cerrada	Responsable
						(Estado inicial: Parcial)	
R-04	Configurar cifrado en nube pública/privada	8.24	8.24	% cifrado en tránsito y reposo	>=95%	GAP: Cláusula 8.24 – Criptografía (Estado inicial: 30%)	Área Infraestructura TI
R-05	Implementar monitoreo continuo de seguridad	8.16	8.16	% alertas críticas atendidas en tiempo	>=90%	GAP: Cláusula 8.16 – Monitoreo (Estado inicial: Parcial)	SOC / Área Seguridad TI

Tabla 22 - Plan de implementación

ID Riesgo	Control aplicado	ISO 27001	ISO 27002	Brecha ISO/MSPI cerrada	Evidencia
R-01	Redundancia en servidores críticos	8.1	8.1	GAP: Cláusula 8.1 – Gestión de activos (Estado inicial: Parcial)	Informe de configuración y pruebas
R-02	Autenticación multifactor habilitada	9.4	9.4	GAP: Cláusula 9.4 – Control de acceso (Estado inicial: No iniciado)	Reporte de cuentas con MFA
R-03	Aplicación de parches críticos	8.8	8.8	GAP: Cláusula 8.8 – Gestión de vulnerabilidades (Estado inicial: Parcial)	Bitácora de actualización
R-04	Cifrado TLS y reposo en nube	8.24	8.24	GAP: Cláusula 8.24 – Criptografía (Estado inicial: 30%)	Informe de auditoría de cifrado
R-05	Monitoreo continuo implementado	8.16	8.16	GAP: Cláusula 8.16 – Monitoreo (Estado inicial: Parcial)	Reporte mensual de alertas

Tabla 23 - Trazabilidad del riesgo

Esta matriz se actualiza trimestralmente y se aprueba en Comité Institucional de Gestión y Desempeño (CIGD).

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

12.3. Anexo 3: Autodiagnósticos y brechas 2025

Este anexo consolida los insumos diagnósticos que fundamentan el PTRSPI, asegurando trazabilidad con el PETI y defendibilidad ante auditoría externa ISO/IEC 27001:2022 y entes de control.

Brecha FURAG / Autodiagnóstico	Riesgo PTRSPI	Control ISO/IEC 27002	KPI / Meta	Evidencia esperada
Cobertura MFA insuficiente	R02: Compromiso de cuentas	8.2 Control de acceso	% cuentas con MFA ≥90%	Reporte plataforma MFA
Vulnerabilidades sin remediación	R03/R06: Vulnerabilidades críticas	8.8 Gestión de vulnerabilidades	% corregidas en SLA ≥95%	Informes escaneo + tickets
Ausencia de cifrado en reposo	R05: Datos sin cifrado	8.24 Criptografía	% cifrado ≥95%	Informe TLS + backup cifrado
Configuración insegura en nube	R04: Configuración insegura cloud	5.23 Seguridad en nube	% cumplimiento línea base ≥90%	Checklist línea base cloud

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

Incumplimiento WCAG 2.1 AA	R08: Accesibilidad	Controles org./tec. aplicables	% conformidad AA ≥95%	Informe validación AA

Tabla 24 - Matriz de brecha → riesgo → control ISO 27002 → KPI/meta → evidencia

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.
BOGOTÁ

12.4. Anexo 4: Plan de Acción proceso gestión de TI 2026

Este documento constituye la fuente única para auditoría y seguimiento del PTRSPI. Todas las actividades, fechas, responsables y entregables se gestionan bajo control documental (ISO 27001:2022, cl. 5.3).

Versión	Fecha	Descripción del cambio	Responsable	Acta Mesa de Trabajo SGSI
1.0	09/01/2026	Inclusión del cronograma operativo 2026	Dirección TIC	Acta No. 001-2026

Tabla 25 - Formato sugerido para el folio de control de versiones

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

13. Control de cambios

Versión	Fecha	Cambio
1.0	23//01/2026	Documento Original aprobado en Comité Institucional de Gestión y Desempeño del 23 de enero de 2026

Nota: El presente plan se aprueba y/o actualiza en el marco del Comité Institucional de Gestión y Desempeño Institucional de la Empresa.

Índice de ilustraciones

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Índice de tablas

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co

Empresa de Renovación Urbana - RenoBo
Carrera 10 No. 17-18. Bogotá - Colombia
@RenoBo_Bogota - www.renobo.com.co