# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## FORTALECIMIENTO DE LAS TIC'S

2026

TERMINAL METROPOLITANA
de Transportes de Barranquilla S.A.

# 1. PRESENTACIÓN

**La Terminal Metropolitana de Transportes de Barranquilla S.A.**, consciente de la importancia estratégica de la información como activo institucional, formula el presente Plan de Seguridad y Privacidad de la Información para la vigencia 2026, con el propósito de fortalecer la gestión del riesgo tecnológico, garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información, y asegurar la continuidad de los servicios soportados por las Tecnologías de la Información.

Este plan se articula con el Plan Estratégico de Tecnologías de la Información – PETI 2026, el Plan Institucional de Acción 2026, el Mapa de Riesgos 2026 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, consolidando un marco integral de planeación, ejecución y seguimiento orientado al fortalecimiento del gobierno de TI y al cumplimiento de los lineamientos de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y el Modelo de Seguridad y Privacidad de la Información (MSPI).

La Oficina de Sistemas lidera la implementación del presente plan, coordinando las acciones técnicas, administrativas y de socialización necesarias para mitigar los riesgos identificados y elevar el nivel de madurez institucional en materia de seguridad de la información.

## 2. OBJETIVO GENERAL

Fortalecer la seguridad y privacidad de la información institucional durante la vigencia 2026 mediante la implementación del Modelo de Seguridad y Privacidad de la Información, la gestión estructurada de riesgos tecnológicos y la ejecución de acciones orientadas a proteger los activos de información, garantizar la continuidad del servicio y mejorar la confianza de las partes interesadas.

## 3. OBJETIVOS ESPECÍFICOS

- Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) como marco de referencia para la gestión de la seguridad.
- Clasificar los activos de información institucionales.
- Elaborar el Análisis de Impacto al Negocio (BIA).
- Diseñar el Plan de Recuperación ante Desastres (DRP).
- Fortalecer la gestión de incidentes tecnológicos mediante el módulo de tickets del sistema ZONA TER.
- Documentar técnicamente la infraestructura, redes y sistemas críticos.
- Asegurar la articulación del plan con el PETI 2026, el Plan Institucional de Acción 2026 y el Mapa de Riesgos 2026.
- Establecer indicadores y mecanismos de seguimiento periódico.

## 4. ALCANCE

El presente plan aplica a todos los sistemas de información, servicios tecnológicos, infraestructura, redes, plataformas, herramientas de soporte y activos de información administrados o soportados por la Oficina de Sistemas, así como a los procesos institucionales que dependen de dichas capacidades tecnológicas para su operación.

Incluye igualmente la interacción con proveedores tecnológicos, el fortalecimiento del módulo de Gestión Documental del sistema ZONA TER y la implementación del módulo de tickets como mecanismo institucional para la atención de solicitudes e incidentes.

## 5. MARCO NORMATIVO

El Plan se fundamenta, entre otros, en:

- Política de Gobierno Digital.
- Modelo Integrado de Planeación y Gestión (MIPG).
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- CONPES de Seguridad Digital.
- Régimen de Protección de Datos Personales.
- Ley de Transparencia y Acceso a la Información Pública.
- Política institucional de administración del riesgo.
- Buenas prácticas ISO/IEC 27001 e ISO/IEC 27005.
- Plan Estratégico Institucional 2024–2027.
- PETI 2026.

## 6. ARTICULACIÓN CON LA PLANEACIÓN INSTITUCIONAL

El Plan de Seguridad y Privacidad de la Información 2026 se articula directamente con:

- PETI 2026: integra las iniciativas de seguridad, arquitectura tecnológica, gobierno de TI y transformación digital.
- Plan Institucional de Acción 2026: las actividades de seguridad forman parte del plan operativo anual.
- Mapa de Riesgos 2026: los riesgos de seguridad de la información alimentan las acciones de tratamiento.
- Plan de Tratamiento de Riesgos 2026: constituye el eje operativo del presente plan.

Esta articulación garantiza coherencia entre estrategia, ejecución y gestión del riesgo.

## 7. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD

- Confidencialidad: acceso restringido únicamente a personal autorizado.
- Integridad: protección contra modificaciones no autorizadas.
- Disponibilidad: acceso oportuno a la información por parte de usuarios autorizados.
- Autenticidad: validación de identidad y perfiles de acceso.
- Trazabilidad: registro de acciones relevantes sobre los sistemas de información.

## 8. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2026

Con base en el Mapa de Riesgos 2026 se identifican, entre otros:

- Filtración o acceso no autorizado a la información.
- Pérdida de información institucional.
- Gestión inadecuada de incidentes tecnológicos.
- Falta de controles técnicos documentados.
- Incumplimiento de lineamientos de transparencia.
- Débil seguimiento a riesgos tecnológicos.

Estos riesgos son gestionados mediante acciones específicas definidas en el Plan de Tratamiento.

## 9. CONTROLES EXISTENTES

Actualmente la entidad cuenta con controles básicos como:

- Antivirus institucional.
- Copias de seguridad periódicas.
- Mecanismos de autenticación de usuarios.
- Administración centralizada de sistemas.
- Gestión documental mediante ZONA TER.

Durante 2026 estos controles serán fortalecidos y formalizados.

## 10. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

Durante la vigencia 2026 se implementará el MSPI como marco estructural, incorporando:

- Clasificación de activos de información.
- Actualización del mapa de riesgos TI.
- Definición de controles técnicos y administrativos.
- Integración con los procesos institucionales.

El resultado será un documento MSPI aprobado y adoptado por la entidad.

## 11. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Se realizará el inventario y clasificación de los activos de información (datos, sistemas, infraestructura y recursos tecnológicos), estableciendo niveles de criticidad y responsables, como insumo para la gestión del riesgo y la continuidad del servicio.

## 12. ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)

Se elaborará el BIA con el fin de identificar procesos críticos, dependencias tecnológicas y tiempos máximos tolerables de interrupción, priorizando la recuperación de servicios esenciales.

# 13. PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP)

Con base en el BIA, se formulará el DRP que definirá procedimientos, roles y responsabilidades para la recuperación de los servicios tecnológicos ante eventos disruptivos.

# 14. GESTIÓN DE INCIDENTES TECNOLÓGICOS

Se implementará el módulo de tickets del sistema ZONA TER como punto central de registro y atención de incidentes, permitiendo trazabilidad, priorización y generación de indicadores de gestión.

# 15. PLAN DE ACCIÓN 2026

| Riesgo | Acción de tratamiento | Responsable | Inicio | Fin | Evidencia |
|---|---|---|---|---|---|
| Filtración o acceso no autorizado | Clasificación de activos de información | Oficina de Sistemas | 01/03/2026 | 30/06/2026 | Matriz de clasificación |
| Filtración o acceso no autorizado | Implementación MSPI | Oficina de Sistemas | 01/04/2026 | 30/09/2026 | Documento MSPI aprobado |
| Pérdida de información | Elaboración BIA | Oficina de Sistemas | 01/05/2026 | 31/07/2026 | Documento BIA |
| Pérdida de información | Elaboración DRP | Oficina de Sistemas | 01/08/2026 | 31/10/2026 | Documento DRP |
| Gestión inadecuada de incidentes | Implementación módulo tickets ZONA TER | Oficina de Sistemas | 01/02/2026 | 30/06/2026 | Módulo operativo y actas |

## 16. INDICADORES

- % de activos clasificados.
- % de avance en implementación del MSPI.
- Elaboración BIA (Sí/No).
- Elaboración DRP (Sí/No).
- % de solicitudes gestionadas mediante ZONA TER.
- % de controles implementados frente a los definidos.

Frecuencia de medición: trimestral y semestral según corresponda.

## 17. SEGUIMIENTO Y MONITOREO

La Oficina de Sistemas realizará seguimiento trimestral a las acciones del plan.

La Oficina de Control Interno efectuará verificación mediante auditorías y revisiones periódicas.

Los resultados se documentarán en informes de seguimiento.

## 18. RESPONSABLES

- Responsable principal: Oficina de Sistemas.
- Apoyo estratégico: Planeación y Control Interno
- Procesos misionales y de apoyo: según área que corresponda.
- Soporte especializado: Proveedores tecnológicos.

## 19. CRONOGRAMA CONSOLIDADO

Las actividades se ejecutarán entre febrero y noviembre de 2026, priorizando en el primer semestre la gestión de incidentes, clasificación de activos y arquitectura, y en el segundo semestre el BIA, DRP, controles y documentación técnica.

## 20. ESTRATEGIA DE SOCIALIZACIÓN

Durante 2026 se realizarán jornadas de socialización dirigidas a funcionarios y contratistas sobre:

- Políticas de seguridad de la información.
- Buenas prácticas de uso de recursos tecnológicos.
- Gestión de incidentes.
- Protección de datos personales.

Las actividades quedarán soportadas mediante actas, correos institucionales y material de capacitación.

## 21. CONCLUSIONES

El Plan de Seguridad y Privacidad de la Información 2026 consolida un enfoque estructurado para la gestión del riesgo tecnológico en la **Terminal Metropolitana de Transportes de Barranquilla S.A.**, articulando estrategia, operación y control.

Su ejecución permitirá avanzar desde un esquema principalmente reactivo hacia un modelo más preventivo y organizado, fortaleciendo el gobierno de TI, la continuidad del servicio y la confianza de las partes interesadas, contribuyendo directamente al cumplimiento de los objetivos institucionales y del PETI 2026.