



SuperTransporte

DOCUMENTO TÉCNICO INSTITUCIONAL

MARZO 2026

Manual de Gestión de Seguridad de la Información

Enfoque: gestión de incidentes de seguridad de la información

Documento técnico fortalecido a partir del procedimiento institucional existente

Entidad / contexto: Superintendencia de Transporte – referencia institucional del documento base analizado

Documento base: Procedimiento "Gestión de Incidentes de Seguridad de la Información", código TIC-PR-013, versión 004

Fecha de elaboración: Marzo de 2026

Naturaleza del documento: Manual formal de referencia, actualización y fortalecimiento técnico

Este manual consolida lineamientos de gobierno, respuesta, continuidad, evidencia, reporte y mejora continua frente a incidentes de seguridad.

Resumen Ejecutivo

El presente documento transforma el procedimiento existente de gestión de incidentes en un manual más completo, formal y utilizable a nivel institucional.

Mantiene los elementos valiosos del documento base como el punto único de contacto a través de la mesa de servicio, la gestión por parte del Oficial de Seguridad de la Información, el escalamiento al CSIRT de Gobierno, la activación del BCP, DRP y CMP, la recolección de evidencia y la retroalimentación mediante lecciones aprendidas y los complementa con un marco de gobierno, criterios de clasificación, controles sobre evidencia, gestión de incidentes con datos personales, indicadores, ANS internos y recomendaciones de mejora.

Marco de Gobierno

Lineamientos formales de gobierno institucional para la gestión de incidentes.

Criterios de Clasificación

Criterios homogéneos para clasificar, priorizar y escalar incidentes.

Controles de Evidencia

Lineamientos de cadena de custodia y preservación de evidencia digital.

Datos Personales

Gestión diferenciada de incidentes con afectación a datos personales.

Indicadores y ANS

Indicadores de gestión y acuerdos de nivel de servicio internos.

1. Introducción

La gestión de incidentes de seguridad de la información es una capacidad esencial para preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizar la continuidad de los servicios institucionales y reducir los impactos operativos, legales, reputacionales y tecnológicos que pueden derivarse de eventos adversos.

En el documento institucional analizado, la gestión inicia con el reporte e identificación del incidente y finaliza con la documentación y las lecciones aprendidas en la herramienta definida por la entidad; asimismo, reconoce la participación de la mesa de servicio, del Oficial de Seguridad de la Información, de los equipos técnicos de OTIC y de los mecanismos de continuidad y reporte a CSIRT de Gobierno.

A partir de dicho insumo, este manual consolida un enfoque más amplio de gestión de seguridad, orientado específicamente a incidentes, con lineamientos de preparación, detección, análisis, contención, erradicación, recuperación, cierre, reporte y mejora continua.

Además, incorpora y actualiza el marco normativo aplicable, corrige referencias institucionales que han sido superadas por disposiciones posteriores y formaliza elementos que conviene fortalecer, tales como la clasificación por severidad, los tiempos internos de respuesta, la gestión de incidentes con datos personales, la cadena de custodia interna y el tratamiento de terceros y proveedores.

2. Objetivos

2.1 Objetivo General

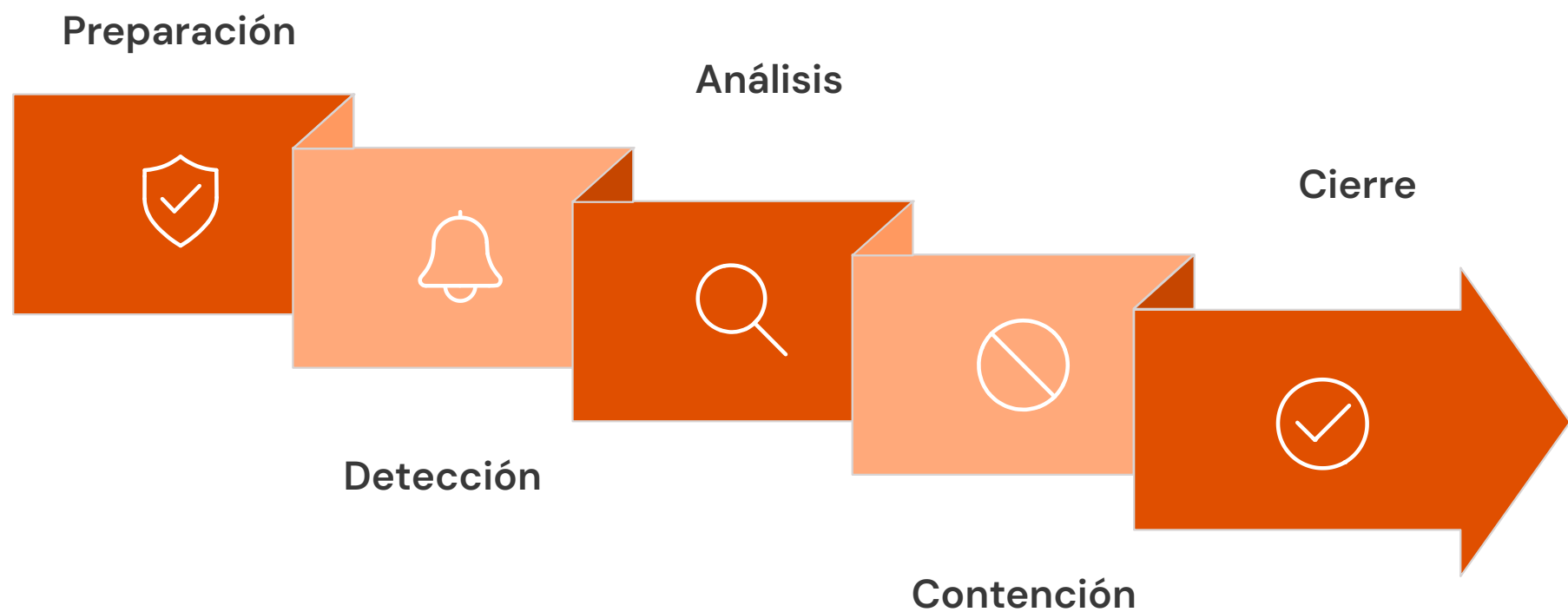
- ❗ Establecer un manual formal de gestión de seguridad de la información, con énfasis en la gestión de incidentes, que permita a la entidad prevenir, detectar, analizar, contener, erradicar, recuperar, documentar y mejorar la respuesta frente a incidentes de seguridad de manera organizada, trazable y alineada con el marco normativo vigente.

2.2 Objetivos Específicos

- Definir roles, responsabilidades y canales de reporte para la atención integral de incidentes.
- Unificar criterios para la clasificación, priorización y escalamiento de incidentes de seguridad de la información y seguridad digital.
- Establecer lineamientos de contención, erradicación, recuperación y retorno controlado a la operación normal.
- Fortalecer la gestión de evidencia, la documentación del caso, la coordinación con terceros y las notificaciones internas y externas.
- Integrar la gestión de incidentes con la continuidad del negocio, la protección de datos personales, la gestión del riesgo y la mejora continua del MSPI y del SGSI institucional.

3. Metodología

La metodología de este manual se estructura sobre el ciclo de vida de gestión de incidentes adoptado por las buenas prácticas de seguridad de la información y alineado con los lineamientos del Modelo de Seguridad y Privacidad de la Información.



El enfoque parte de una fase de preparación institucional; continúa con detección y reporte; incluye análisis, clasificación y priorización; desarrolla acciones de contención, erradicación y recuperación; y concluye con el cierre formal, la comunicación a partes interesadas y la incorporación de lecciones aprendidas al ciclo PHVA y a la gestión de riesgos.

Desde la perspectiva operativa, se conservan las trece actividades identificadas en el procedimiento institucional analizado, pero se reorganizan como un manual para facilitar su uso por parte de líderes, equipos técnicos, auditores y responsables de control. La metodología incorpora tres criterios adicionales de fortalecimiento:

1. **Respuesta basada en severidad y criticidad.**
2. **Gestión diferenciada cuando exista afectación a datos personales, continuidad del negocio o terceros.**
3. **Mejora continua obligatoria mediante indicadores, causa raíz y actualización de controles.**

4. Marco Normativo y de Referencia Aplicable

El presente manual fue elaborado considerando la normatividad colombiana principal aplicable a entidades públicas en materia de seguridad de la información, gobierno digital, protección de datos, transparencia, continuidad y seguridad digital. El cuadro siguiente sintetiza las referencias normativas más relevantes para la gestión de incidentes y para el fortalecimiento del documento institucional existente.

Instrumento	Aplicación al manual
Ley 1273 de 2009	Tipifica conductas relacionadas con la protección de la información y de los datos; es la base penal para incidentes con posible relevancia delictiva.
Ley 1341 de 2009	Define principios y conceptos del sector TIC y sirve de marco general para la organización de las tecnologías de la información y las comunicaciones.
Ley 1581 de 2012	Establece el régimen general de protección de datos personales; es relevante para incidentes que involucren pérdida, acceso no autorizado, alteración o divulgación de datos personales.
Decreto 1377 de 2013 y Decreto 1074 de 2015	Desarrollan y compilan la reglamentación asociada al tratamiento de datos personales, incluyendo obligaciones de responsables y encargados.
Ley 1712 de 2014 y Decreto 103 de 2015	Regulan transparencia y acceso a la información pública; obligan a distinguir entre información pública, clasificada, reservada y restringida durante la gestión del incidente.

4. Marco Normativo (continuación)

Instrumento	Aplicación al manual
Decreto 1078 de 2015	Compila el régimen del sector TIC y sirve como marco reglamentario para política digital, seguridad digital y disposiciones complementarias.
CONPES 3995 de 2020	Fija la Política Nacional de Confianza y Seguridad Digital y orienta el fortalecimiento de capacidades institucionales y de gobernanza.
Resolución 500 de 2021 – MinTIC	Adopta lineamientos generales del MSPI, lineamientos y estándares de seguridad digital y el procedimiento general para la gestión de incidentes de seguridad digital.
Decreto 338 de 2022	Fortalece la gobernanza de la seguridad digital, crea instancias y exige medidas técnicas, humanas y administrativas para la gestión y respuesta a incidentes.
Decreto 767 de 2022	Establece los lineamientos generales de la Política de Gobierno Digital y fija responsabilidades institucionales para su implementación y mejora continua.
Resolución 2277 de 2025 – MinTIC	Actualiza el Anexo 1 de la Resolución 500 de 2021, fortalece el MSPI y alinea los lineamientos con ISO/IEC 27001:2022.
Resolución 5095 de 2024 – Superintendencia de Transporte	Actualiza la Política General de Seguridad y Privacidad de la Información de la entidad y deroga la Resolución 7386 de 2022; por tanto, toda referencia institucional debe adecuarse a esta actualización.
Documento Maestro del MSPI y lineamientos de roles, indicadores y riesgo	Sirven como referencia técnica para roles, información documentada, mejora continua, medición y articulación con el SGSI.

SECCIÓN 5

5. Alcance y Lineamientos Rectores del Manual

5.1 Alcance

Este manual aplica a todos los procesos, dependencias, funcionarios, contratistas, terceros, sistemas de información, servicios en la nube, bases de datos, redes, estaciones de trabajo, aplicaciones, servicios expuestos a internet, proveedores tecnológicos, activos de información y recursos que administren, transmitan, procesen o custodien información institucional.

- ❗ Incluye eventos e incidentes originados por causas internas o externas, accidentales o deliberadas, siempre que puedan comprometer la seguridad de la información o la continuidad del servicio.

5.2 Principios Rectores

Oportunidad

Todo evento sospechoso deberá reportarse y atenderse sin demoras injustificadas.

Trazabilidad

Toda actuación debe quedar registrada de manera suficiente, verificable y oportuna.

Confidencialidad

La información del incidente se compartirá solo con quienes tengan necesidad funcional o legal de conocerla.

Integridad de la Evidencia

Las evidencias deben preservarse de manera que mantengan valor técnico, administrativo y eventualmente judicial.

Proporcionalidad

Las medidas aplicadas deben responder al nivel de riesgo, criticidad e impacto del incidente.

Coordinación

La atención del incidente no es exclusiva del área de TI; requiere articulación con procesos misionales, jurídicos, comunicaciones, talento humano, control interno y terceros, según corresponda.

Mejora Continua

Cada incidente debe generar información útil para reforzar controles, sensibilización, procedimientos y decisiones de inversión en seguridad.

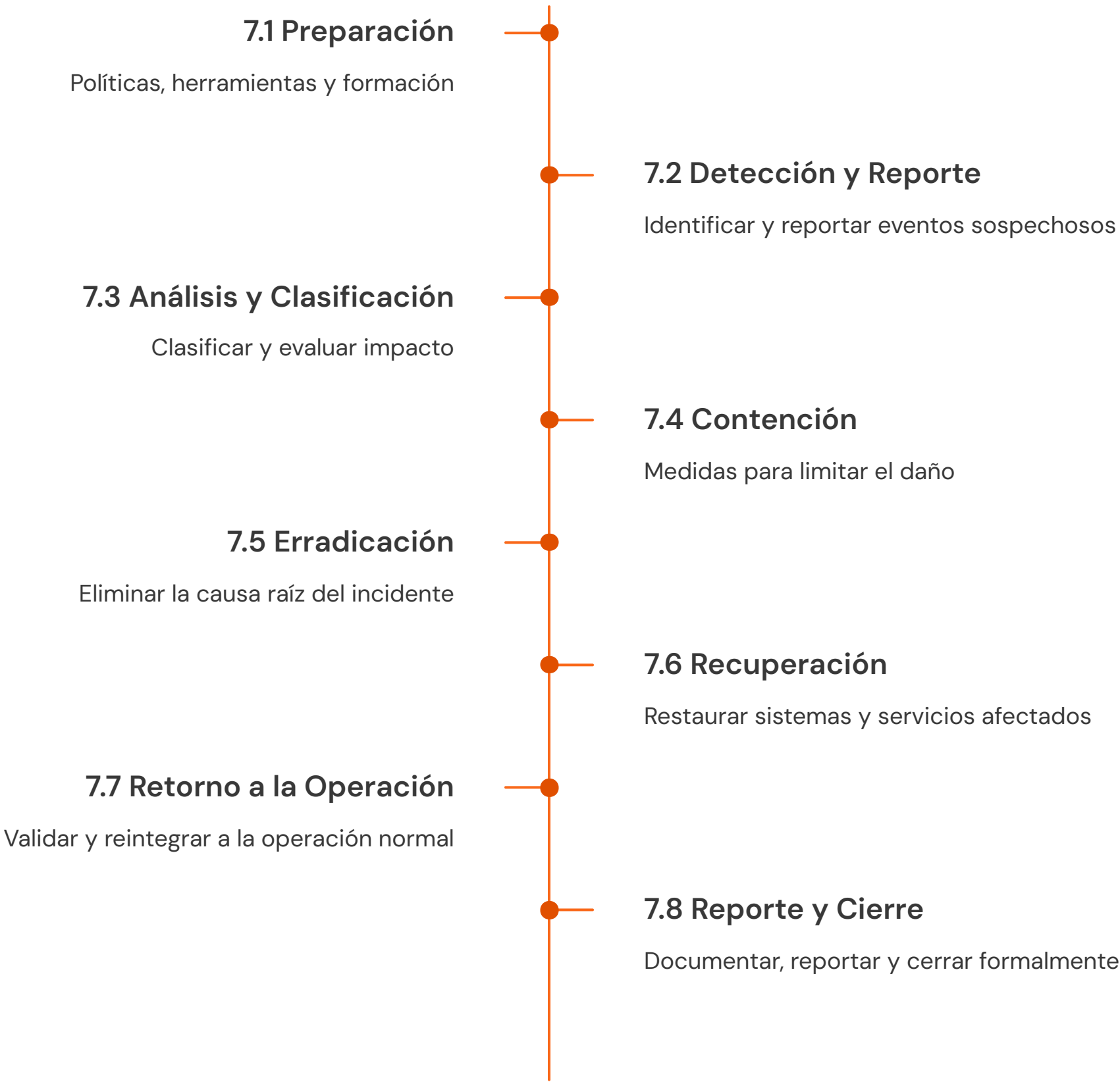
6. Roles y Responsabilidades

La siguiente tabla define los roles institucionales y sus responsabilidades principales en la gestión de incidentes de seguridad de la información.

Rol	Responsabilidad principal
Mesa de servicio / primer nivel	Recibir el reporte, registrar el caso, validar información mínima, categorizar preliminarmente y escalar según impacto y prioridad.
Oficial de Seguridad de la Información	Dirigir el análisis del incidente, reclasificarlo, coordinar la respuesta, decidir el escalamiento, activar mesas técnicas, consolidar el reporte y validar el cierre.
Equipos de infraestructura, sistemas de información y desarrollo	Ejecutar contención, erradicación, recuperación, validación técnica y retorno controlado a la operación.
Jefe de OTIC / liderazgo TIC	Aprobar decisiones de alto impacto, coordinar recursos y apoyar la activación de continuidad, crisis o contratación especializada cuando aplique.
Líder del proceso afectado	Definir impacto funcional, colaborar en priorización, validar restablecimiento y apoyar comunicaciones a usuarios y partes interesadas.
Jurídica, control interno y comunicaciones	Participar cuando existan implicaciones legales, disciplinarias, reputacionales, contractuales o de vocería institucional.
Terceros y proveedores	Atender oportunamente los incidentes asociados a servicios bajo su responsabilidad y entregar evidencias, informes técnicos y soportes.
Todos los funcionarios y contratistas	Reportar de inmediato eventos sospechosos, preservar la información y abstenerse de manipular evidencia sin autorización.

7. Procedimiento de Gestión de Incidentes

La secuencia operativa del presente manual toma como punto de partida las actividades ya definidas en el procedimiento institucional, pero las desarrolla con mayor precisión para facilitar su aplicación como guía formal de gestión. Las fases mínimas son las siguientes:



A continuación se desarrolla cada una de las fases del procedimiento de gestión de incidentes de seguridad de la información.

7.1 Preparación

- ❗ La entidad debe mantener responsables designados, canales de reporte, formatos de incidente, inventario de activos críticos, criterios de clasificación, respaldos, mecanismos de monitoreo, matrices de contacto, procedimientos de continuidad, lineamientos de evidencia y sensibilización periódica.



Responsables designados

Roles claramente asignados con canales de reporte y formatos de incidente definidos.



Inventario de activos críticos

Criterios de clasificación, respaldos y mecanismos de monitoreo activos.



Procedimientos de continuidad

Matrices de contacto, lineamientos de evidencia y sensibilización periódica del personal.

7.2 Detección y Reporte

Todo funcionario, contratista, proveedor o tercero que detecte un evento sospechoso debe reportarlo inmediatamente a la mesa de servicio o al canal institucional definido.

 Se debe registrar fecha, hora, fuente, síntoma, usuario afectado, activo comprometido y cualquier evidencia inicial disponible.

7.3 Análisis y Clasificación

El primer nivel examina el evento y el Oficial de Seguridad define si existe un incidente, su categoría, alcance, severidad, posibles causas, afectación de servicios, necesidad de escalar a proveedores y pertinencia de reporte al CSIRT de Gobierno.

7.4 Contención

Se aplican medidas inmediatas para evitar propagación o incremento del impacto:

Aislamiento

Aislamiento de equipos comprometidos.

Credenciales

Revocación de credenciales comprometidas.

Segmentación

Segmentación de red afectada.

Servicios

Suspensión temporal de servicios cuando aplique.

Bloqueo

Bloqueo de indicadores maliciosos y control de accesos.

7.5 Erradicación

Una vez controlado el incidente, deben eliminarse artefactos maliciosos, puertas de acceso, configuraciones inseguras o vulnerabilidades explotadas. Esta fase incluye parchado, rotación de contraseñas, reforzamiento de controles y validaciones técnicas.

7.6 Recuperación

Comprende la restauración de los sistemas y servicios afectados, la verificación de integridad, la validación funcional por parte del proceso afectado y el seguimiento reforzado para confirmar que el incidente no persista.

7.7 Retorno a la Operación Normal

 El regreso a producción debe ser controlado, documentado y aprobado según criticidad. No debe darse por cerrado un caso únicamente porque el servicio volvió a operar; se requiere validar causa, controles y riesgos residuales.

7.8 Reporte, Cierre y Lecciones Aprendidas

La gestión concluye con el informe del incidente, la comunicación a partes interesadas, el cierre en la herramienta oficial, la identificación de la causa raíz, el registro de lecciones aprendidas y la actualización de controles, configuraciones, políticas o capacitaciones.

8. Clasificación, Criticidad y Tiempos Internos de Respuesta

Se recomienda que la entidad formalice una matriz de criticidad complementaria a la utilizada en mesa de servicio, de manera que exista un criterio homogéneo para incidentes de seguridad de la información, seguridad digital y continuidad. La siguiente tabla puede adoptarse como referencia de trabajo:

Nivel	Criterio orientador	ANS inicial	Lineamiento
Crítico	Afecta servicio esencial, múltiples dependencias, infraestructura crítica, datos sensibles o exposición pública de alto impacto.	Atención inmediata	Escalamiento máximo en 30 minutos y decisión inmediata sobre continuidad, reporte y mesa técnica.
Alto	Afecta un proceso relevante, varios usuarios o compromete credenciales, integridad de datos o disponibilidad significativa.	Hasta 2 horas	Seguimiento intensivo, coordinación con OTIC y evaluación de reporte externo según categoría.
Medio	Impacto controlado, contenido en un área o sistema sin indisponibilidad general ni afectación masiva.	Hasta 8 horas hábiles	Atención prioritaria y documentación completa del caso.
Bajo	Evento aislado o de bajo impacto, sin afectación material relevante a la operación.	Hasta 24 horas hábiles	Gestión normal, con análisis para prevenir recurrencia.

8. Clasificación — Visualización de Niveles de Criticidad



9. Gestión de Evidencia y Cadena de Custodia Interna

El documento base ya incorpora la recolección y análisis de evidencia. No obstante, para fortalecer su utilización institucional, se recomienda establecer de manera expresa que toda evidencia digital o documental asociada a un incidente deberá ser identificada, preservada, almacenada y transferida con trazabilidad.

La evidencia podrá incluir:

Registros de auditoría

Logs y bitácoras de sistemas y redes.

Correos y capturas

Correos electrónicos y capturas de pantalla relevantes.

Imágenes forenses

Imágenes forenses y artefactos maliciosos identificados.

Reportes de monitoreo

Respaldos, reportes de monitoreo y declaraciones de usuarios.

Comunicaciones

Comunicaciones con proveedores y terceros involucrados.

La manipulación de evidencia deberá limitarse al personal autorizado. Cuando el incidente pueda tener connotación disciplinaria, contractual, administrativa o penal, deberá documentarse la cadena de custodia interna, el responsable de cada transferencia y la justificación de cada acceso. En casos graves o de alto impacto, la entidad podrá requerir servicios especializados de análisis forense digital o peritaje técnico, tal como ya se contempla en la versión vigente del procedimiento base.

SECCIÓN 10

10. Gestión de Incidentes con Datos Personales, Terceros y Continuidad

Incidentes con Datos Personales

Cuando un incidente involucre datos personales, la entidad deberá tratarlo simultáneamente como incidente de seguridad y como evento relevante en materia de protección de datos. Esto implica:

- Verificar el tipo de dato afectado y la cantidad de titulares.
- Evaluar el riesgo material para los derechos de las personas.
- Determinar la exposición o acceso no autorizado.
- Cumplir las obligaciones de reporte o gestión frente a la autoridad competente.
- Adoptar medidas de contención y comunicación orientadas a minimizar afectaciones adicionales.

10. Gestión con Terceros y Continuidad del Negocio

Incidentes con Terceros o Proveedores

Si el incidente compromete servicios prestados por terceros o proveedores, estos deberán ser activados conforme a sus ANS y obligaciones contractuales, exigiéndose evidencia técnica, diagnóstico, tiempos de solución y medidas correctivas.

Activación de Planes de Continuidad

Si existe impacto sobre continuidad, el Oficial de Seguridad y la Jefatura de OTIC deberán activar la mesa técnica correspondiente y valorar la activación del:

- **BCP** – Plan de Continuidad de Negocio
- **DRP** – Plan de Recuperación ante Desastres
- **CMP** – Plan de Manejo de Crisis

Tal como ya lo prevé el documento base.

11. Notificación, Reporte y Cierre Formal

Contenido del Reporte Interno

El reporte interno del incidente debe consolidar:

La línea de tiempo y los activos comprometidos.

1

2

El impacto y la causa presunta o confirmada.

Las medidas de contención, erradicación y recuperación.

3

4

La evidencia disponible y la intervención de terceros.

Las decisiones de continuidad y las comunicaciones realizadas.

5

Cuando la categoría o severidad lo requiera, deberá notificarse al CSIRT de Gobierno o a la instancia que corresponda, siguiendo los lineamientos vigentes del MSPI y del marco de gobernanza de seguridad digital.

11. Condiciones para el Cierre Formal del Incidente

 El cierre del incidente no podrá efectuarse mientras existan acciones técnicas pendientes, evidencias sin organizar, reportes incompletos o controles pendientes de implementación.

El caso debe cerrarse únicamente cuando se cumplan todas las siguientes condiciones:



12. Indicadores y Mejora Continua

La gestión de incidentes debe medirse para apoyar decisiones de mejora, priorización y presupuesto. Se recomienda adoptar como mínimo los siguientes indicadores:

- Número de incidentes por categoría.
- Número de incidentes por severidad.
- Tiempo promedio de detección.
- Tiempo promedio de contención.
- Tiempo promedio de recuperación.

- Porcentaje de incidentes cerrados dentro del ANS.
- Número de incidentes repetitivos.
- Número de incidentes con participación de proveedores.
- Incidentes con afectación a datos personales.
- Porcentaje de acciones correctivas implementadas.

-
- ✓ Las lecciones aprendidas deberán retroalimentar la gestión de riesgos institucionales, la sensibilización del personal, los controles técnicos, los procedimientos, los acuerdos con terceros y la actualización del MSPI y del SGSI. De esta forma, la atención del incidente deja de ser reactiva y se convierte en un insumo de madurez institucional.

13. Principales Mejoras Incorporadas Frente al Documento Base

Manual formal con enfoque de gobierno

Se convierte el procedimiento operativo en un manual formal, con enfoque de gobierno, operación, evidencia y mejora continua.

Marco normativo actualizado

Se actualiza el marco normativo, incorporando la Resolución 2277 de 2025 y la política institucional vigente de la Superintendencia de Transporte contenida en la Resolución 5095 de 2024, que derogó la Resolución 7386 de 2022.

Distinción conceptual fortalecida

Se distinguen con mayor claridad los conceptos de evento, incidente, incidente mayor, incidente con datos personales e incidente con afectación a continuidad del negocio.

Principios, roles y tiempos definidos

Se definen principios rectores, roles, severidad, tiempos internos de respuesta y criterios para cierre formal.

Gestión de evidencia fortalecida

Se fortalece la gestión de evidencia y la cadena de custodia interna.

Componente de indicadores y seguimiento

Se agrega un componente de indicadores y seguimiento, necesario para auditoría, madurez y mejora continua.

Coordinación interinstitucional explícita

Se deja explícita la coordinación con procesos jurídicos, control interno, comunicaciones, talento humano y terceros cuando la naturaleza del caso lo requiera.

Ejercicios periódicos de simulación

Se recomienda programar ejercicios periódicos de simulación y revisión del procedimiento para comprobar su eficacia operacional.

14. Conclusión

El procedimiento institucional de gestión de incidentes de seguridad de la información analizado presenta una base adecuada y operativamente útil; sin embargo, para efectos de adopción, auditoría, capacitación y estandarización institucional, resultaba conveniente transformarlo en un manual más robusto, formal y alineado con la normatividad vigente.

El presente documento cumple ese propósito al organizar el ciclo de atención, consolidar los roles, reforzar la continuidad, la evidencia, el reporte, la protección de datos personales y la mejora continua.



Se recomienda que este manual sea revisado por OTIC, Jurídica, Control Interno y el Comité Institucional de Gestión y Desempeño, con el fin de validar su adopción formal, armonizarlo con los formatos vigentes de la entidad y actualizar, cuando corresponda, los procedimientos, matrices de criticidad, ANS, mecanismos de comunicación y compromisos contractuales con terceros.

15. Fuentes Normativas y Documentales Consultadas

Las siguientes fuentes normativas y documentales fueron consultadas para la elaboración del presente manual:

Procedimiento institucional base

Superintendencia de Transporte. Procedimiento "Gestión de Incidentes de Seguridad de la Información", código TIC-PR-013, versión 004, aprobado el 22 de septiembre de 2025.

Leyes de protección de información y TIC

Ley 1273 de 2009. Protección de la información y de los datos. — Ley 1341 de 2009. Principios y conceptos sobre la sociedad de la información y la organización de las TIC. — Ley 1581 de 2012. Régimen general de protección de datos personales.

Decretos reglamentarios

Decreto 1377 de 2013 y Decreto 1074 de 2015. Reglamentación y compilación del tratamiento de datos personales. — Ley 1712 de 2014 y Decreto 103 de 2015. Transparencia y acceso a la información pública. — Decreto 1078 de 2015. Decreto Único Reglamentario del Sector TIC.

Política Nacional y Gobernanza Digital

CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital. — Decreto 338 de 2022. Gobernanza de la seguridad digital. — Decreto 767 de 2022. Política de Gobierno Digital.

Resoluciones MinTIC y Superintendencia de Transporte

Resolución 500 de 2021 del Ministerio TIC. Lineamientos y estándares para la estrategia de seguridad digital y adopción del MSPI. — Resolución 5095 de 2024 de la Superintendencia de Transporte. Actualización de la Política General de Seguridad y Privacidad de la Información. — Resolución 2277 de 2025 del Ministerio TIC. Actualización del Anexo 1 de la Resolución 500 de 2021 y fortalecimiento del MSPI.

Documento Maestro del MSPI

Documento Maestro del Modelo de Seguridad y Privacidad de la Información – MSPI, versión 2025, y lineamientos asociados de roles, indicadores y riesgo.

Información del Documento

Datos de Identificación

Título: Manual de Gestión de Seguridad de la Información

Código de referencia: TIC-PR-013, versión 004

Fecha de elaboración: Marzo de 2026

Entidad: Superintendencia de Transporte

Naturaleza y Uso

Manual formal de referencia, actualización y fortalecimiento técnico.

Documento elaborado en formato de informe técnico-formal para uso institucional.

Revisión recomendada por:

- Oficina de Tecnologías de la Información y las Comunicaciones (OTIC)
- Oficina Jurídica
- Control Interno
- Comité Institucional de Gestión y Desempeño

Este manual consolida lineamientos de gobierno, respuesta, continuidad, evidencia, reporte y mejora continua frente a incidentes de seguridad. Su adopción formal deberá ser validada por las instancias institucionales competentes.