



SuperTransporte

INFORME TÉCNICO INSTITUCIONAL

FASE 6 · MARZO 2026

Superintendencia de Transporte Informe de Seguimiento y Control — Fase 6

Análisis consolidado de los documentos entregados: **Manual de Respuesta a Incidentes (IRP)** y **Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR)**

Documento	Fase evaluada	Entregables revisados	Fecha
Informe formal de seguimiento y control	Fase 6	Manual IRP y Plan BC/DR	Marzo de 2026

El presente informe tiene como propósito documentar el seguimiento y control efectuado en la fase 6, en la cual se presentaron dos instrumentos estratégicos orientados al fortalecimiento de la seguridad de la información, la continuidad operativa y la capacidad de respuesta institucional frente a eventos adversos: el **Manual de Respuesta a Incidentes de Seguridad de la Información** y el **Plan de Continuidad del Negocio y Recuperación ante Desastres**.

Introducción

En el marco del proceso de seguimiento y control correspondiente a la fase 6, se revisaron dos documentos de alta relevancia para la madurez institucional en materia de seguridad de la información y resiliencia operativa. El primero corresponde al **Manual de Gestión de Seguridad de la Información con enfoque en gestión de incidentes**, el cual consolida lineamientos de gobierno, reporte, contención, recuperación, manejo de evidencia y mejora continua frente a incidentes de seguridad. El segundo es el **Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR)**, orientado a proteger, respaldar, verificar y recuperar servicios críticos soportados por Veeam Backup y un appliance de 200 TB.

Primer entregable

Manual de Gestión de Seguridad de la Información con enfoque en gestión de incidentes: gobierno, reporte, contención, recuperación, manejo de evidencia y mejora continua.

Segundo entregable

Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR): protección, respaldo, verificación y recuperación de servicios críticos soportados por Veeam Backup y un appliance de 200 TB.

Ambos documentos evidencian una línea de fortalecimiento institucional enfocada en la prevención, atención y recuperación frente a eventos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. De igual manera, muestran una articulación coherente con buenas prácticas de seguridad digital, continuidad del negocio, trazabilidad de la evidencia, gestión del riesgo y cumplimiento normativo, aspectos que resultan esenciales para una entidad que debe garantizar estabilidad operativa, confianza institucional y capacidad de respuesta ante escenarios de afectación tecnológica.

En este contexto, el presente informe sintetiza el alcance de los dos entregables, resalta sus componentes más relevantes y deja constancia de su pertinencia para la institución, no solo como documentos de cumplimiento, sino como herramientas de gestión que permiten ordenar responsabilidades, fortalecer procesos, formalizar decisiones y mejorar la capacidad institucional para enfrentar incidentes de seguridad y situaciones de indisponibilidad o pérdida de información.

Objetivos

2.1 Objetivo general

Presentar un informe formal de seguimiento y control de la fase 6, consolidando el análisis de los documentos entregados —Manual de Respuesta a Incidentes (IRP) y Plan de Recuperación/Continuidad de Datos BC/DR—, con el fin de evidenciar su aporte al fortalecimiento de la seguridad de la información, la continuidad operativa y la capacidad institucional de recuperación.

2.2 Objetivos específicos

1**Describir el Manual IRP**

Describir de manera ejecutiva el contenido y propósito del Manual de Respuesta a Incidentes presentado en la fase 6.

2**Resumir el Plan BC/DR**

Resumir los componentes técnicos, operativos y de gobierno incluidos en el Plan BC/DR entregado para la protección y recuperación de la información.

3**Identificar complementariedad**

Identificar la complementariedad entre ambos documentos como parte de una estrategia integral de respuesta, continuidad y recuperación.

4**Valor institucional**

Dejar constancia del valor institucional de estos entregables para la mejora del control interno, la trazabilidad operativa, el cumplimiento normativo y la resiliencia tecnológica.

SECCIÓN 3

Documentos presentados en la Fase 6

A continuación se relacionan los dos documentos revisados en el marco del seguimiento y control de la fase 6, con su enfoque principal y aporte institucional:

No.	Documento	Enfoque principal	Aporte institucional
1	Manual de Respuesta a Incidentes (IRP)	Gestión integral de incidentes de seguridad de la información.	Define roles, flujo de atención, severidad, evidencia, escalamiento y mejora continua.
2	Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR)	Protección, respaldo, verificación y recuperación de servicios críticos.	Fortalece la resiliencia operativa, la restauración verificable y la continuidad institucional.

Resumen del Manual de Respuesta a Incidentes (IRP)

El Manual de Respuesta a Incidentes presentado en la fase 6 constituye un instrumento formal orientado a organizar la gestión de incidentes de seguridad de la información desde una perspectiva institucional. El documento no se limita a la reacción técnica ante un evento adverso, sino que incorpora una visión integral que contempla gobierno, preparación, detección, análisis, clasificación, contención, erradicación, recuperación, cierre y lecciones aprendidas. De esta manera, el manual convierte el tratamiento de incidentes en un proceso trazable, ordenado y medible.



Ciclo de gestión de incidentes

Diez fases clave para la respuesta organizada.

Dentro de sus principales fortalezas se encuentra la definición de roles y responsabilidades, la participación de la mesa de servicio, del Oficial de Seguridad de la Información, de los equipos técnicos y de las instancias de apoyo institucional, así como la articulación con mecanismos de continuidad, escalamiento y reporte. También resulta relevante la incorporación de criterios de criticidad, tiempos de respuesta, gestión de evidencia, tratamiento de incidentes asociados a datos personales y la necesidad de retroalimentar el sistema mediante acciones correctivas y mejora continua.

- ⚠ Desde el punto de vista de seguimiento y control, este documento aporta valor porque establece un marco de actuación claro ante incidentes, reduce la improvisación operativa, facilita la toma de decisiones, fortalece la trazabilidad de cada caso y mejora la coordinación entre las áreas involucradas. Asimismo, permite que la entidad avance hacia una mayor madurez en seguridad digital al tratar los incidentes no solo como eventos técnicos aislados, sino como situaciones que pueden afectar la operación, la reputación, el cumplimiento legal y la confianza sobre la gestión institucional.

Componentes destacados del Manual IRP

Roles y responsabilidades

Definición de la participación de la mesa de servicio, del Oficial de Seguridad de la Información, de los equipos técnicos y de las instancias de apoyo institucional.

Criterios de criticidad y tiempos de respuesta

Incorporación de criterios de criticidad y tiempos de respuesta para priorizar la atención de incidentes según su impacto.

Gestión de evidencia

Lineamientos para el tratamiento, preservación y cadena de custodia de la evidencia asociada a cada incidente.

Datos personales e incidentes asociados

Tratamiento específico de incidentes asociados a datos personales, en línea con el cumplimiento normativo vigente.

Mejora continua

Necesidad de retroalimentar el sistema mediante acciones correctivas y mejora continua derivadas de cada incidente gestionado.

Escalamiento y reporte

Articulación con mecanismos de continuidad, escalamiento y reporte hacia instancias internas y externas según la severidad del evento.

Resumen del Plan de Continuidad del Negocio y Recuperación ante Desastres (BC/DR)

El Plan BC/DR entregado en esta fase se orienta a la protección de la información y a la recuperación controlada de servicios críticos soportados por **Veeam Backup** y por un **appliance de 200 TB** destinado al almacenamiento de copias de seguridad. Su enfoque es amplio y técnicamente sólido, pues reconoce que la continuidad del negocio no consiste únicamente en disponer de respaldos, sino en garantizar que estos sean seguros, verificables, recuperables y útiles en un escenario real de contingencia o desastre.

Aspectos clave desarrollados en el Plan BC/DR



- ✓ En términos institucionales, el BC/DR fortalece la capacidad de recuperación ante fallas tecnológicas, pérdida de datos, errores operativos, ransomware o indisponibilidad de infraestructura. Su relevancia es alta porque transforma el respaldo de información en una capacidad real de continuidad y resiliencia, permitiendo que la entidad no solo conserve copias, sino que tenga un marco formal para restablecer procesos esenciales, reducir tiempos de interrupción, mitigar impactos reputacionales y dar soporte a una gestión más segura y confiable de los activos críticos.

Articulación entre el IRP y el BC/DR

Uno de los hallazgos más importantes de la fase 6 es que los dos documentos presentados no operan de manera aislada, sino que se complementan de forma estratégica. El **Manual IRP** fortalece la capacidad de detectar, analizar y responder ante incidentes de seguridad de la información, mientras que el **Plan BC/DR** proporciona el marco técnico y operativo para recuperar servicios y datos cuando el impacto del incidente supera la contención inicial o compromete la continuidad de la operación.

Manual IRP

Ayuda a responder con oportunidad, coordinación y control ante incidentes de seguridad de la información.

- Detección y análisis
- Respuesta organizada
- Contención y erradicación
- Trazabilidad de actuaciones

Plan BC/DR

Asegura que exista una ruta clara para restaurar capacidades, validar integridad y retornar a la normalidad operacional con menores niveles de riesgo.

- Recuperación de servicios y datos
- Validación de integridad
- Reanudación de la operación
- Reducción de riesgos residuales

Esta relación es especialmente valiosa porque permite cubrir dos dimensiones críticas de la gestión institucional: por un lado, la respuesta organizada frente a un incidente; por otro, la recuperación efectiva y la reanudación de la operación.

La existencia simultánea de ambos documentos fortalece el ecosistema de control interno, mejora la gobernanza de seguridad de la información y aporta una base documental robusta para auditoría, seguimiento, toma de decisiones y mejora continua. Esto refleja una visión más madura y preventiva de la gestión tecnológica, alineada con la necesidad de proteger tanto la información como la continuidad de los servicios institucionales.

Conclusión

Como resultado del seguimiento y control de la fase 6, se evidencia que los documentos presentados constituyen insumos de alto valor para la institución. El **Manual de Respuesta a Incidentes** fortalece la capacidad de reacción organizada frente a eventos de seguridad, ordena responsabilidades, mejora la trazabilidad de las actuaciones y facilita una atención más oportuna, coherente y documentada. Por su parte, el **Plan BC/DR** robustece la continuidad operativa al establecer lineamientos claros para la protección, verificación y recuperación de la información y de los servicios críticos, lo cual incrementa la resiliencia institucional frente a fallas, ataques o situaciones de desastre.

En conjunto, estos documentos son buenos y convenientes para la entidad porque contribuyen a consolidar una cultura de preparación, respuesta y recuperación basada en procedimientos formales, criterios técnicos, responsabilidades definidas y mecanismos de mejora continua. Su adopción y uso permiten fortalecer la seguridad digital, reducir la improvisación ante eventos adversos, elevar el nivel de control sobre los activos de información, respaldar el cumplimiento normativo y generar mayor confianza en la capacidad de la institución para sostener y restablecer su operación.

Herramientas estratégicas de gestión

Más que entregables documentales, el IRP y el BC/DR deben entenderse como herramientas estratégicas de gestión. Su implementación progresiva, revisión periódica y articulación con los procesos institucionales pueden convertirse en un factor determinante para mejorar la gobernanza, la madurez operativa y la capacidad de respuesta de la entidad frente a riesgos de seguridad de la información y de continuidad del negocio.

Cierre del Informe

Se deja constancia de que, dentro de la fase 6, los documentos revisados aportan una base técnica y metodológica favorable para el fortalecimiento de la seguridad de la información, la continuidad de los servicios y la recuperación institucional ante eventos disruptivos.

Seguridad de la información Base técnica y metodológica favorable para el fortalecimiento de la seguridad de la información.	Continuidad de los servicios Marco formal para garantizar la continuidad de los servicios institucionales ante eventos adversos.	Recuperación institucional Capacidad de recuperación institucional ante eventos disruptivos, fallas tecnológicas o situaciones de desastre.
--	--	---

Documento	Informe formal de seguimiento y control — Fase 6
Entidad	Superintendencia de Transporte
Entregables revisados	Manual IRP y Plan BC/DR
Fecha	Marzo de 2026
Estado	Informe de seguimiento y control completado — Fase 6 cerrada