

UNIDAD DE  
AUDITORÍA  
INTERNA

VIALIDAD  
NACIONAL

# AUDITORÍA DE PLAN DE CONTINGENCIA

Informe Definitivo N° 26

PLAN 2016

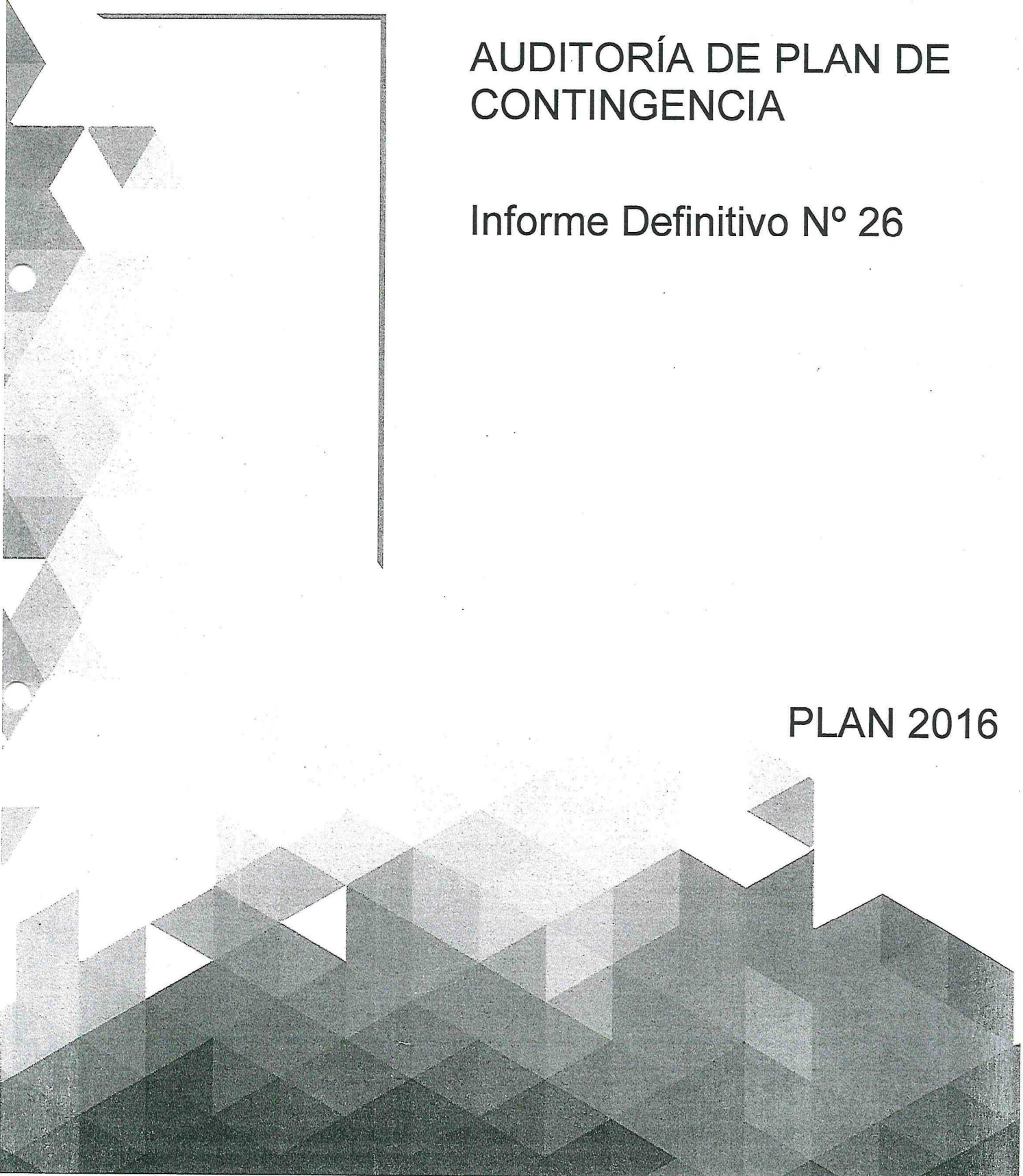


TABLA DE CONTENIDOS

INFORME EJECUTIVO	3
INFORME ANALITICO	5
OBJETO	5
ALCANCE	5
TAREA REALIZADA	5
ANTECEDENTES	6
MARCO NORMATIVO	6
OTROS ANTECEDENTES	6
MARCO DE REFERENCIA	7
ACLARACIONES PREVIAS	7
HALLAZGOS Y RECOMENDACIONES	8
CONCLUSIÓN GENERAL	13

*del*  
*2012*  
*Jin*

## INFORME EJECUTIVO

El presente Informe se elaboró con el objeto de verificar que los planes de contingencia contemplen un conjunto de procedimientos y de recursos necesarios para la continuidad de las operaciones ante interrupciones inesperadas y posterior recuperación a la actividad normal, en los cuales estén involucrados todas las áreas y servicios del Organismo, y se mantengan los mismos debidamente actualizados.

Un plan de contingencias es un instrumento fundamental para el manejo de las Tecnologías de la Información y Comunicaciones, que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones del Organismo.

De acuerdo a lo establecido por Resolución DNV N° 1917/06, se remitió las áreas auditadas el correspondiente Informe Preliminar con las observaciones halladas, para que emita su descargo dentro de los 10 días hábiles de recibido el mismo. No habiendo emitido las áreas auditadas opinión, esta Unidad de Auditoría Interna otorga carácter de Informe Definitivo al Preliminar, entendiendo que los auditados se encuentran de acuerdo con las observaciones y recomendaciones formuladas.

Las tareas de campo se desarrollaron en la sede de Casa Central de la Dirección Nacional de Vialidad (DNV), en el período mayo-diciembre de 2016, de conformidad con la metodología que la Sindicatura General de la Nación tiene establecida en las Normas Generales de Control Interno y las Normas de Auditoría Interna Gubernamental.

De la labor de auditoría realizada se constató que la conformación del Comité de Seguridad de la Información del Organismo se encuentra desactualizada respecto a los cambios en el ejercicio de funcionarios, no evidenciándose en consecuencia el cumplimiento de las funciones que le fueron conferidas por Resolución DNV N° 1740/2006.

Consecuentemente, el Organismo no tiene definida una Política de Seguridad de la Información, el cual es un componente clave de los sistemas de control interno cuyo propósito es gestionar el riesgo. Asimismo no cuenta con un Plan de Contingencias aprobado, instrumento necesario para garantizar la continuidad de las operaciones.

En lo que respecta a la Subgerencia de Informática y Transmisión de Datos (SITD), cabe destacar que inició un proyecto de Política de Seguridad de la Información y elaboró un Plan de Contingencia, con algunas debilidades, ambos sin revisión del Comité de Seguridad de la Información y aprobación formal.

En cuanto a la muestra seleccionada de los Planes de Contingencia de Distritos, se verificó que no fueron confeccionados conforme a la "Guía para la elaboración de un Plan de Continuidad de las actividades" impartidas por la SITD. Los mismos principalmente presentan debilidades en la descripción de los procedimientos a realizar durante o inmediatamente después de materializada una amenaza, y de los que se deben llevar a cabo para restaurar el estado de las cosas tal como se encontraban antes de la materialización de la amenaza.

Cabe destacar que la mayoría de las observaciones para su regularización requieren la colaboración de diversas áreas del Organismo, por lo cual las medidas deberían arbitrarse fundamentalmente por parte del Comité de Seguridad de la Información.

*[Handwritten signature]*

## CONCLUSIÓN GENERAL


En el marco de la labor de auditoría realizada, se concluyó que resulta necesario implementar una serie de mejoras a efectos de fortalecer el sistema de control interno imperante, lo cual se encuentra evidenciado en los hallazgos detectados por esta Unidad de Auditoría Interna.

Por lo expuesto, se recomienda al Administrador General la actualización de los representantes del Comité de Seguridad de la Información conforme a la Decisión Administrativa N° 669/2004, y al citado Comité la adopción de las acciones necesarias tendientes a regularizar las observaciones planteadas, lo cual contribuirá a fortalecer el ambiente de control en esta Dirección Nacional.

Buenos Aires, 10 de abril de 2017.

*del*  
*2017*

  
Ing. GABRIELA CRUZ  
Coordinadora Área Sistemas - UAI  
Dirección Nacional de Vialidad

  
Cra. VALERIA NAVARIDAS  
Auditora Adjunta de Gestión de  
Recursos y Áreas de Apoyo - UAI  
Dirección Nacional de Vialidad

  
Cr. MARCELO GUILLERMO BIANCHI  
AUDITOR INTERNO - U.A.I.  
DIRECCIÓN NACIONAL DE VIALIDAD

**INFORME ANALITICO****OBJETO**

Verificar que los planes de contingencia contemplen un conjunto de procedimientos y de recursos necesarios para la continuidad de las operaciones ante interrupciones inesperadas y posterior recuperación a la actividad normal, en los cuales estén involucradas todas las áreas y servicios del Organismo, y se mantengan los mismos debidamente actualizados.

**ALCANCE**

Las tareas de campo se desarrollaron en el período mayo-diciembre de 2016, de conformidad con las Normas de Auditoría Interna Gubernamental (Resolución SGN N° 152/02), el Manual de Auditoría Interna Gubernamental (Resolución SGN N° 3/11).

Estas labores comprendieron la revisión del plan de contingencias y de otros documentos, que también contemplan procedimientos que se aplican antes, durante y después de la materialización de una amenaza. Todos estos instrumentos fueron elaborados por la Subgerencia de Informática y Transmisión de Datos (SITD), y carecen de aprobación formal.

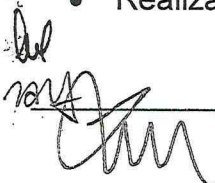
En tal sentido, fueron solicitados a los Distritos sus Planes de Contingencias, a fin de corroborar que los mismos se adecúen al lineamiento impartido por la SITD. A tal efecto, se seleccionó una muestra y se analizó la documentación confeccionada por los siguientes Distritos:

- 4° Mendoza
- 5° Salta
- 6° Jujuy
- 7° Santa Fe
- 8° La Rioja
- 11° Catamarca
- 13° Chubut
- 16° Santiago del Estero
- 22° Formosa

**TAREA REALIZADA**

La labor de auditoría consistió en la aplicación de procedimientos generales, los cuales se detallan a continuación:

- Realización de cuestionarios y entrevistas en las áreas auditadas.



- Análisis del plan de contingencia elaborado por la Subgerencia de Informática y Transmisión de Datos, de los registros en uso y la documentación respaldatoria de los procedimientos efectuados en cada etapa respecto a la materialización de cualquier amenaza.
- Relevamiento de documentación e información relativa a Políticas de Seguridad de la Información y Comité de Seguridad de la Información.
- Verificación de la correcta aplicación de la normativa vigente.

Asimismo, entre otros, fueron realizados los siguientes procedimientos específicos de control:

- Análisis de los controles preventivos establecidos para evitar la materialización de una amenaza.
- Evaluación de las medidas instauradas para aplicarse durante la materialización de una amenaza, o inmediatamente después, a fin de atenuar sus efectos adversos.
- Análisis de los procedimientos para restaurar las actividades del Organismo tal y como se encontraban antes de su interrupción.
- Comprobación de la existencia de copias de seguridad de la información.
- Revisión de una prueba de restauración de la base de datos de un sistema, a partir del backup realizado por personal informático.

## **ANTECEDENTES**

---

### **MARCO NORMATIVO**

---

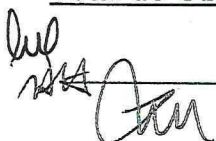
- Decisión Administrativa N° 669/2004 de Jefatura de Gabinete de Ministros. Establece que los organismos del Sector Público Nacional deberán dictar o adecuar sus políticas de seguridad y conformar un Comité de Seguridad de la Información.
- Disposición N° 1/2015 de Jefatura de Gabinete de Ministros – Oficina Nacional de Tecnologías de la Información. Aprueba las Políticas de Seguridad de la Información Modelo para Organismos de la Administración Pública Nacional.
- Resolución DNV N° 1740/2006. Crea y conforma el Comité de Seguridad de la Información en el Organismo, además establece sus funciones.
- Resolución DNV N° 11/2009. Cambia los funcionarios que integran el Comité de Seguridad de la Información.

### **OTROS ANTECEDENTES**

---

**Informe UAI N° 32/2009 "Auditoría a Planes de Contingencias".**

**Total de Observaciones:** 7, las cuales se encuentran pendientes de regularización.



**Informe UAI N° 58/2013 "Auditoría de Backup".**

Total de Observaciones: 3, las cuales se encuentran pendientes de regularización.

**Informe UAI N° 40/2014 "Aspectos de Control de la Tecnología Informática".**

Total de Observaciones: 2, las cuales se encuentran pendientes de regularización.

Todas estas observaciones se encuentran reformuladas en el presente Informe.

## MARCO DE REFERENCIA

### ACLARACIONES PREVIAS

Los activos o recursos, humanos, materiales e inmateriales (software, conocimiento acumulado, etc.) que dispone la DNV para alcanzar los objetivos definidos se encuentran en un entorno de incertidumbre, que en ocasiones puede provocar interrupciones inesperadas. Muchas de estas interrupciones suelen ser temporales, y las condiciones vuelven a normalizarse en un período que no ocasiona situaciones críticas para la actividad normal del Organismo. No obstante, puede haber circunstancias que generen interrupciones prolongadas, que llegan a influir en la capacidad de funcionamiento de los servicios o impiden el desarrollo normal de los mismos.

Para prever las consecuencias de estas situaciones y definir las estrategias que aseguren la continuidad de la actividad en el menor tiempo y con el menor trastorno posible, es necesaria la elaboración de un Plan de Contingencias. Este plan debería comprender:

- **Plan de respaldo.** Contempla las contramedidas preventivas antes de que se materialice una amenaza con el fin de evitarla.
- **Plan de emergencia.** Contempla los procedimientos para ser ejecutados durante la materialización de una amenaza, con la finalidad de atenuar sus efectos adversos.
- **Plan de recuperación.** Contempla las medidas necesarias después de materializada y controlada la amenaza. Su objetivo es reestablecer las operaciones tal como se encontraban antes de la materialización de la misma.

En resumen, un Plan de Contingencias es un instrumento fundamental para el manejo de las Tecnologías de la Información y Comunicaciones, que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones del Organismo.

*[Handwritten signature]*

## HALLAZGOS Y RECOMENDACIONES

---

- 1. El Comité de Seguridad de la Información creado, conformado y modificado por Resoluciones DNV N° 1740/2006 y N° 11/2009 se encuentra desactualizado, y no se evidencia el cumplimiento de sus funciones.**

**Impacto: Alto**

El Comité de Seguridad de la Información creado y conformado por Resolución DNV N° 1740/2006, posteriormente modificado por Resolución DNV N° 11/2009, se encuentra desactualizado respecto a los cambios en el ejercicio de funcionarios de esta DNV, dado que aún se encuentra conformado por varios agentes que no pertenecen más a la Repartición o que no están ejerciendo los cargos jerárquicos respectivos.

Además, no se evidencia el cumplimiento de las funciones que le fueron asignadas por Resolución al citado Comité.

### Recomendación

En relación a la reestructuración organizativa que se vienen desarrollando en el Organismo, resulta necesario renovar a los representantes del Comité de Seguridad de la Información conforme a la Decisión Administrativa JGM N° 669/2004. Asimismo se recomienda que el citado Comité ejerza sus funciones, todas ellas referentes a aspectos de seguridad en el Organismo.

- 2. La DNV no tiene definida una Política de Seguridad de la Información.**

**Impacto: Alto**

El Organismo no posee una Política de Seguridad de la Información aprobada formalmente, componente clave de los sistemas de control interno, cuyo propósito es gestionar el riesgo.

Por su parte la Subgerencia de Informática y Transmisión de Datos elaboró un proyecto y generó el "Expediente N° 3126/2007 s/Política de Seguridad de la Información del Comité de Seguridad de la DNV", para gestionar su evaluación y aprobación, sin embargo aún no cuenta con la anuencia del Comité y la máxima autoridad del Organismo.

### Recomendación

Tal como fuera recomendado en el hallazgo anterior resulta necesario renovar el Comité de Seguridad, el cual conforme a sus funciones deberá examinar el proyecto citado para hacer las correcciones necesarias y elevarlo a la máxima autoridad para su aprobación.

A tal fin, se deberán considerar los aspectos sugeridos en el *Modelo de Política de Seguridad de la Información para la Administración Pública* aprobado por Disposición N° 1/2015 de Jefatura de Gabinete – Oficina Nacional de Tecnologías de Información.

*[Handwritten signature]*



Complementariamente se recomienda que la política a aprobar se encuentre alineada con el umbral de riesgo tolerable definido por el Organismo, y una vez aprobada sea actualizada periódicamente.

### 3. El Organismo no dispone de un Plan de Contingencias aprobado.

**Impacto: Medio**

Conforme al relevamiento efectuado, la Subgerencia de Informática y Transmisión de Datos dispone de un Plan de Contingencias y procedimientos documentados, en los que se describen algunos métodos para enfrentar eventuales situaciones que afecten los recursos informáticos. Sin embargo, dicho Plan no fue revisado por el Comité de Seguridad ni aprobado por la máxima autoridad del Organismo.

#### Recomendación

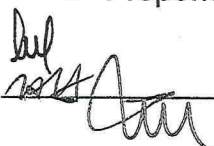
Esta Unidad recomienda que una vez renovado el Comité de Seguridad de la Información, éste se encargue de revisar el Plan de Contingencia generado por la Subgerencia de Informática y Transmisión de Datos, proponer las modificaciones necesarias, y elevar a la máxima autoridad para su aprobación.

También debería examinarse toda otra documentación que describa acciones a emprender una vez ocurrido un incidente que coloque en peligro la continuidad de los servicios de procesamiento de información del Organismo, como por ejemplo el "*Protocolo de Contingencia Eléctrica*".

Asimismo, es importante identificar los controles preventivos implementados, como por ejemplo el sistema de supresión de fuego instalado en sala de servidores, las copias de resguardo de información realizadas por Subgerencia de Informática y Transmisión de Datos, etc.

Considerando que el citado Comité tiene a su cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información frente a interrupciones imprevistas, además de lo antedicho deberá realizar las siguientes tareas:

- Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en término de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción pueda tener en la actividad del Organismo.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar las actualizaciones periódicas de los planes y procesos implementados.
- Proponer las modificaciones a los planes de contingencia.



#### 4. El Plan de Contingencia iniciado por la Subgerencia de Informática y Transmisión de Datos presenta algunas deficiencias.

**Impacto: Medio**

El Plan de Contingencia documentado por la Subgerencia de Informática y Transmisión de Datos presenta algunas deficiencias:

- En caso de desastre total se menciona trasladar los servicios al sitio de procesamiento de datos alternativo, pero no detalla su ubicación, como así tampoco los servicios a ser trasladados, ni las personas encargadas de realizarlo.
- Los procedimientos no describen claramente las acciones a emprender una vez ocurrido un incidente que coloque en peligro las operaciones del Organismo. Por ejemplo, en fs. 175 dice: *"En caso de desastre total y/o hasta contar con equipamiento y software de base instalado dentro o fuera del edificio se realizarán aquellas tareas que no se puedan suspender, manualmente"*, pero no se detallan cuáles son esas tareas ni como se realizarán.
- No describe los responsables de la ejecución de cada uno de los componentes del Plan y las vías de contacto posibles.
- Separadamente del Plan, existen otros documentos que describen acciones a emprender una vez ocurrido un incidente que coloque en peligro las operaciones del Organismo.
- No se encuentran formalmente acordados los tiempos de recuperación para los servicios críticos.
- No se definió un cronograma de mantenimiento que especifique cómo y cuándo será probado el Plan, y el proceso para el mantenimiento del mismo.

#### Recomendación

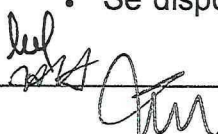
El Comité de Seguridad de la Información deberá considerar las falencias mencionadas precedentemente y proponer las modificaciones necesarias para subsanarlas. Además, se recomienda elaborar un presupuesto asociado al Plan de Contingencia a fin de asegurar su viabilidad económica.

#### 5. El procedimiento para realizar las copias de seguridad de la información (backup) presenta algunas deficiencias.

**Impacto: Medio**

El procedimiento de backup como respaldo frente a eventualidades presenta ciertas falencias que podrían entorpecer la recuperación de la información en el caso de pérdida de la copia original, como ser:

- Se dispone de una sola unidad lectrograbadora, necesaria para restaurar las



copias de resguardo de la información, por lo cual en caso de dañarse este dispositivo no podría recuperarse las copias.

- El Organismo posee sólo una licencia del software utilizado para realizar la restauración de la información, por lo que no está contemplada la instalación del software en otro equipo alternativo.
- Los catálogos de las copias de resguardo se almacenan en el servidor y no en las unidades extraíbles LTO-2, esto genera una dependencia del servidor, y en caso que falle imposibilita recuperar la información de las copias.

Además se presentan las siguientes consideraciones:

- El rótulo de las copias de seguridad no coincide con lo dispuesto en el *Manual de Funciones, Normas y Procedimientos Internos - SITD*.
- Los armarios de guardados de las copias de seguridad se comparten con otros elementos, y el nivel de protección física no resulta suficiente.
- Respecto a las pruebas de restauración de backup presenciadas por esta Unidad, no está documentado todo el proceso de recuperación.

### Recomendación

Adoptar las medidas pertinentes para proveer al personal informático de por lo menos una unidad lectograbadora y una licencia de software adicionales, a fin de garantizar la recuperación de la información en caso de dañarse el dispositivo mencionado o el equipamiento en el cual se encuentra instalado el software.

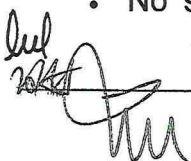
A los encargados de realizar las copias de seguridad se recomienda almacenar los catálogos en las unidades extraíbles LTO-2, documentar el proceso de restauración de backup e incrementar el nivel de protección física de las copias de resguardo.

### 6. Planes de Contingencias de Distritos presentan deficiencias.

**Impacto: Medio**

En la muestra de los Planes de Contingencia de Distritos seleccionada se verificó que los mismos no fueron confeccionados conforme a la "*Guía para la elaboración de un Plan de Continuidad de las actividades*" impartidas por la SITD. Consecuentemente, en algunos de ellos se presentan las siguientes consideraciones:

- Falta detallar procedimientos que indiquen como el personal debe continuar sus tareas en caso que un imprevisto interrumpa la actividad normal.
- No se determinan los responsables de llevar adelante las tareas, para los siniestros evaluados.
- No se describen de forma precisa las acciones a llevarse a cabo para la



recuperación de la actividad normal.

- No cuentan con cronogramas de mantenimiento, que indiquen cómo y cuando se probarán.

### Recomendación

El Comité de Seguridad de la Información deberá revalidar o establecer una nueva "Guía para la elaboración de un Plan de Continuidad de las actividades", a fin de que cada Distrito readecue su Plan de Contingencias.

En base a ello, personal informático y responsables de la información de cada Distrito, deberán realizar las modificaciones pertinentes al Plan y elevarlo al citado Comité para la evaluación y posterior aprobación del mismo. Además, se deberán evaluar las necesidades que presenta cada Distrito e instrumentar los medios para proveerlos de recursos (hardware, software, etc.) necesarios para garantizar el resguardo de la información y la continuidad de las operaciones.

del  
del  
del

## CONCLUSIÓN GENERAL

El presente Informe se elaboró con el objeto de verificar la existencia de planes de contingencia y de continuidad o de recuperación de la actividad ante desastres, en los que estén involucradas todas las áreas y servicios del Organismo, y que se mantengan los mismos debidamente actualizados.

En el marco de la labor de auditoría realizada, se concluyó que resulta necesario implementar una serie de mejoras a efectos de fortalecer el sistema de control interno imperante, lo cual se encuentra evidenciado en los hallazgos detectados por esta Unidad de Auditoría Interna.

Cabe destacar que la mayoría de las observaciones para su regularización requieren la colaboración de diversas áreas del Organismo, por lo cual las medidas deberían arbitrase fundamentalmente por parte del Comité de Seguridad de la Información.

Por lo expuesto, se recomienda a la Administración General renovar los representantes del Comité conforme a la Decisión Administrativa JGM N° 669/2004, y al Comité la adopción de las acciones necesarias tendientes a regularizar las observaciones planteadas, lo cual contribuirá a fortalecer el sistema de control interno imperante en el Organismo.

Buenos Aires, 10 de abril de 2017.

*del*  
*2017*

Ing. GABRIELA CRUZ  
Coordinadora Área Sistemas - UAI  
Dirección Nacional de Vialidad

Cra. VALERIA NAVARIDAS  
Auditora Adjunta de Gestión de  
Recursos y Áreas de Apoyo - UAI  
Dirección Nacional de Vialidad

Cr. MARCELO GUILLERMO BIANCHI  
AUDITOR INTERNO - U.A.I.  
DIRECCIÓN NACIONAL DE VIALIDAD