



# **Plan de Contingencias Logísticas**

**2013/2014**

**Oficina de Planeación  
Bogotá D.C.**



## Contenido

INTRODUCCIÓN .....	4
CAPÍTULO I. LA ADMINISTRACIÓN DE CONTINGENCIAS EN LA PROCURADURÍA GENERAL DE LA NACIÓN .....	9
1.1 OBJETIVO .....	9
1.2 VENTAJAS POTENCIALES .....	9
1.3 ALCANCE .....	9
1.4. ORGANIZACIÓN INSTITUCIONAL PARA LA ADMINISTRACIÓN DE RIESGOS Y CONTINGENCIAS .....	11
1.4.1 Comité Directivo .....	11
1.4.2 Coordinadores de los planes y programas de contingencias .....	13
1.4.3 Grupos de desarrollo de los planes de emergencia y contingencia .....	13
1.4.3.1 Equipo de Atención de Emergencias. ....	14
1.4.3.2 Equipo de Evaluación de Daños. ....	14
1.4.3.3 Equipo de Seguimiento y Control. ....	14
1.5 PROCESO GENERAL DE CONTINGENCIA .....	15
1.5.1 SIMULACROS .....	16
CAPÍTULO II. MARCO TEÓRICO .....	18
2.1. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS .....	21
2.1.1. Riesgos externos .....	22
2.1.2. Riesgos internos .....	24
CAPÍTULO III. SUSPENSIÓN DE SERVICIOS PÚBLICOS .....	27
3.1. Definición .....	27
3.2. Procedimiento .....	27
3.3. Procedimiento en caso de suspensión de agua, energía y teléfono o recolección de basuras .....	27
3.4. SUSPENSIÓN POR INCUMPLIMIENTO EN LOS PAGOS A LOS PRESTADORES DE SERVICIOS .....	29
CAPÍTULO IV. DESABASTECIMIENTO DE SUMINISTRO DE ELEMENTOS DE OFICINA Y DE TRABAJO .....	31
4.1. Definición .....	31
4.2. Procedimientos .....	31
CAPÍTULO V. DAÑO MEMORIA INSTITUCIONAL - ARCHIVO .....	33
5.1. Definición .....	33
5.2. Procedimientos .....	33
5.3. Implantación de soluciones .....	35



CAPITULO VI. PLAN DE CONTINGENCIAS LOGÍSTICAS INFORMÁTICAS PCLI	
.....	36
6.1. Objetivos.....	36
6.2. Alcance .....	36
6.3. Fases del Plan.....	37
6.3.1. Identificación de requerimientos.....	37
6.3.2. Análisis de Riesgos - Análisis de vulnerabilidades e impactos de las contingencias.....	42
6.3.3. Desarrollo.....	44
6.4. Emergencia y Recuperación .....	44
6.5. Prueba .....	49
6.5.1 General.....	49
6.5.2 Específicos:.....	49
6.6. Administración y Mantenimiento.....	50



## INTRODUCCIÓN

Las condiciones de cambios constantes en las que se ven envueltas las organizaciones, son marcadas por procesos complejos, dinámicos e inciertos, sobre los cuáles se debe actuar constantemente en procura de poder responder y adaptarse a los nuevos requerimientos del entorno.

El Plan de Contingencias Logísticas se constituye en un instrumento para dar respuesta oportuna, adecuada y coordinada a situaciones de emergencia causadas por fenómenos destructivos de origen natural o humano.

Teniendo en cuenta la vulnerabilidad en las sedes de la PGN, el Plan de Contingencias Logísticas sirve para atender oportunamente con personal capacitado y con los apoyos institucionales a los riesgos de origen (naturales, tecnológicos, biológicos, químicos, físicos y sociales), que se determinen ex ante, durante o ex post de cada situación posible.

Sin embargo, es fundamental contar con la suma del esfuerzo de todos, cuya composición permita fortalecer y cumplir en tiempo, las acciones tendientes a prevenir y mitigar desastres en modo y tiempo de las circunstancias señaladas y dar respuesta oportuna a la sociedad dentro de un marco de seguridad.

El objetivo del presente documento es delimitar funciones, actividades y responsabilidades de las dependencias, para que de forma conjunta y coordinada actúen ante la presencia o inminencia de algún agente perturbador, que ponga en riesgo su estructura física y que no permita el cumplimiento de las funciones asignadas a la Entidad.

La Oficina de Planeación ha actualizado el Plan de Contingencias logísticas, de manera que sirva como marco de acción institucional para prevenir, atender y restablecer la normalidad en situaciones de perturbación o pérdida.

El Plan de Contingencias Logísticas es el documento que describe el diseño de un nuevo esquema de gestión, que cohesione a las personas en procura de la misión de la PGN.

El Plan de Contingencia Logística permite mantener la continuidad de las operaciones, ante la ocurrencia de alguna falla que provoque la paralización parcial o total de la Entidad. Este abarca desde la recuperación de aquellos servicios y recursos críticos ante eventos que van desde desastres naturales



(terremotos, inundaciones, etc.) hasta no naturales (el daño en un computador, el agotamiento de la papelería de la entidad, fallas técnicas y/o errores de programas, etc.).

El Plan de Contingencia Logística de la Procuraduría General de la Nación, se encuentra establecido en Decreto Ley 262 de 2000, en el Artículo 11, numeral (6) “Diseñar el plan de contingencias logísticas de la entidad”, como función de la Oficina de Planeación.

En la Ley 87 de 1993, Artículo 2º. “Objetivos del sistema de Control Interno” hace referencia a los principios. Constitucionales que debe caracterizar la administración pública, el diseño y el desarrollo del Sistema de Control Interno se orientarán al logro de los siguientes objetivos fundamentales:

**a.** Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que lo afecten;

**f.** Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.



## Factores de Riesgo – Bogotá D.C. Nivel Central

FACTORES DE RIESGOS																									
NIVEL CENTRAL	AUSENCIA DE FLUIDO ELÉCTRICO			SUSPENSIÓN SERVICIO TELEFÓNICO			CORTE EN EL SERVICIO DE AGUA			POSIBLE MAL FUNCIONAMIENTO DEL SOFTWARE O HARDWARE			DESABASTECIMIENTO DE INSUMOS Y SUMINISTROS			PERDIDA INFORMACIÓN HISTÓRICA LOS DOCUMENTOS DE ARCHIVO CENTRAL.									
	NIVEL DE RIESGO	PROCE- DIMIEN- TOS CON- TROL ES	REQUIER- MIEN- TOS	NIVEL DE RIESGO	PROCE- DIMIEN- TOS CON- TROL ES	REQUIER- MIEN- TOS	NIVEL DE RIESGO	PROCE- DIMIEN- TOS CON- TROL ES	REQUIER- MIEN- TOS	NIVEL DE RIESGO	PROCE- DIMIEN- TOS CON- TROL ES	REQUIER- MIEN- TOS	NIVEL DE RIESGO	PROCE- DIMIEN- TOS CON- TROL ES	REQUIER- MIEN- TOS	NIVEL DE RIESGO	PROCE- DIMIEN- TOS CON- TROL ES	REQUIER- MIEN- TOS							
NIVEL DE RIESGO	Alto	Medio	Bajo	Sí	Sí	Sí	Alto	Medio	Bajo	Sí	Sí	Sí	Alto	Medio	Bajo	Sí	Sí	Sí	Alto	Medio	Bajo	Sí	Sí	Sí	
<b>TORRE A</b>																									
Sótanos Parquaderos																									
Piso 1 Lobby																									
Piso 4 Auditorios y salas																									
Piso 5 Sistemas																									
Pisos 2/3																									
Pisos 6/15																									
Pisos 16/28																									
<b>TORRE B</b>																									
Centro Atención Público																									
Pisos 2/3 Oficinas																									
piso 3 Biblioteca																									
Piso 4 comunica Torre A																									
<b>TORRE C</b>																									
Auditorio																									
Piso 2/3/4 Oficinas																									
<b>TORRE MANUEL MEJÍA</b>																									
Sótanos Parquaderos																									
Piso 1 Lobby/2																									
Pisos 4/10 oficinas																									

**FLUIDO ELÉCTRICO:** Daño técnico por actos vandálicos, sobrecarga de líneas de transmisión y mantenimientos programados y subestaciones.

**SERVICIO TELÉFONICO:** Robo de la infraestructura de los operadores de servicio y daños masivos en redes de fibra.

**SERVICIO DE AGUA:** Daño Técnico debido a mantenimiento de la infraestructura perímetro 2K y robo de infraestructura.

**SISTEMAS:** Al ampliar nuestra red de telefonía IP a 40 nuevas sedes, la planta de telefonía a nivel central se saturó y hubo intermitencia en el servicio.

**SUMINISTROS:** El riesgo es casi nulo debido a que la PGN es muy cumplida con el pago a sus proveedores

**ARCHIVO:** Saturado por espacio físico, pendiente traslado nueva sede.



## Factores de Riesgo – Nivel Territorial

		FACTORES DE RIESGOS																													
DEPENDENCIAS REGIONALES	NIVEL DE RIESGO	AUSENCIA DE FLUIDO ELECTRICO					SUSPENSION SERVICIO TELEFONICO					CORTE EN EL SERVICIO DE AGUA					POSIBLE MAL FUNCIONAMIENTO DEL SOFTWARE O HARDWARE					DESABASTECIMIENTO DE INSUMOS Y SUMINISTROS					PERDIDA INFORMACIÓN HISTÓRICA LOS DOCUMENTOS DE ARCHIVO CENTRAL.				
		Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO					
1	REGIONAL DE ANTIOQUIA	Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO	Alto	Medio	Bajo	SI	NO					
2	REGIONAL DE ARAUCA																														
3	REGIONAL DEL ATLÁNTICO																														
4	REGIONAL DEL AMAZONAS																														
5	REGIONAL DE BOLIVAR																														
6	REGIONAL DE BOYACÁ																														
7	REGIONAL DE CALDAS																														
8	REGIONAL DE CAQUETÁ																														
9	REGIONAL DE CASANARE																														
10	REGIONAL DE CAUCA																														
11	REGIONAL DEL CESAR																														
12	REGIONAL DE CHOCÓ																														
13	REGIONAL DE CORDOBA																														
14	REGIONAL CUNDINAMARCA																														
15	REGIONAL DE GUAVIARE																														
16	REGIONAL DE LA GUAJIRA																														
17	REGIONAL DEL HUILA																														
18	REGIONAL DE MAGDALENA																														
19	REGIONAL DEL META																														
20	REGIONAL DE NARIÑO																														
21	REGIONAL DE QUINDIO																														
22	REGIONAL N. SANTANDER																														
23	REGIONAL DE PUTUMAYO																														
24	REGIONAL SAN ANDRÉS																														
25	REGIONAL DE RISARALDA																														
26	REGIONAL DE SANTANDER																														
27	REGIONAL DE SUCRE																														
28	REGIONAL DE TOLIMA																														
29	REGIONAL DE VAUPES																														
30	REGIONAL DEL GUAINIA																														
31	REGIONAL VALLE CAUCA																														
32	REGIONAL DEL VICHADA																														

**FLUIDO ELÉCTRICO:** Riesgo medio por cuanto existe una supervisión permanente del coordinador o responsable;

Revisión y reparación (preventivo y correctivo) por parte de la correspondiente electrificadora y se minimiza el riesgo.

**SERVICIO TELEFÓNICO:** Riesgo medio al contar con voz IP en varias Regionales y Provinciales presentándose saturación.

**SERVICIO DE AGUA:** Riesgo medio por cuanto se realizan revisiones técnicas periódicas por parte de la empresa de acueducto y alcantarillado.

**SISTEMAS:** Riesgo medio por que se reporta inmediato a Oficina de Sistemas, y se hacen las revisiones técnicas y mantenimiento preventivo por parte de la empresa contratista, en las sedes con UPS los riesgos son bajos y se cuenta con procedimientos y controles.



SUMINISTROS: Falta de contrato suscrito con el proveedor Outsourcing, falta de suministros de oficina en el nivel central.

ARCHIVO: El riesgo es medio porque hay supervisión y verificación periódica para mejorar las condiciones físicas del sitio, y se efectúan controles por parte de la Regional y los funcionarios han tomado nota de las recomendaciones para mejorar.



# **CAPÍTULO I. LA ADMINISTRACIÓN DE CONTINGENCIAS EN LA PROCURADURÍA GENERAL DE LA NACIÓN**

## **1.1 OBJETIVO**

El objetivo específico es organizar a la Procuraduría General de la Nación para prevenir y atender las contingencias logísticas.

## **1.2 VENTAJAS POTENCIALES**

La organización de la PGN a través del PCL, tiene ventajas potenciales que ayudan a prevenir o disminuir el impacto de los siniestros:

Identificar los riesgos potenciales a que están expuestos, los procedimientos, documentos, sistemas de información y las sedes.

Generar una cultura de seguridad y control en todas las dependencias y sedes de la Entidad.

Asegurar la estabilidad operativa de la Procuraduría General frente a la ocurrencia de un siniestro de impacto negativo para la organización.

Medir el grado de seguridad de los mecanismos adoptados para afrontar los riesgos con probabilidad de ocurrencia alto en la Entidad a Nivel Nacional, a través de la elaboración de panoramas de riesgos acompañados por las autoridades competentes.

## **1.3 ALCANCE**

El documento identifica los riesgos potenciales a los que esta sometida la PGN y sobre los cuáles se deben definir acciones preventivas, así como las áreas y personas responsables de su elaboración, socialización y actualización y es uno de los instrumentos estratégicos de gestión para el manejo de riesgos.

El cuadro siguiente muestra los diferentes documentos que tienen relación con el manejo del riesgo en la Entidad.



RIESGOS	DOCUMENTO	DEPENDENCIA RESPONSABLE
Naturales (Terremoto, maremotos, inundaciones, etc.)	Plan de emergencias	Grupo de Bienestar Social Integral
Incendios		
Atentado terrorista (Explosivos, biológico, francotirador, etc.)	Manual de seguridad de instalaciones	División de Seguridad
Toma de instalaciones		
Asonada o alteración social		
Seguridad de personas	Manual de esquemas de seguridad (capítulo incluido en el manual de seguridad)	
Emergencias de salud	Cartilla de primeros auxilios	Grupo de Bienestar Social Integral
Accidentes de trabajo Accidentes de tránsito Falla de ascensores Aneagaciones Daño de instalaciones (Caída de techos, paredes, puertas, escaleras, etc.)	Manual de seguridad industrial	Grupo de Bienestar Social Integral, División Administrativa
Contaminaciones biológicas o químicas	Manual de seguridad Ambiental	Delegada de Asuntos Ambientales y Agrarios
Suspensión de servicios públicos	Plan de Contingencias Logísticas	Oficina de Planeación, División Administrativa
Desabastecimiento de elementos de oficina		Oficina de Planeación, División de Documentación
Daño memoria institucional, archivo		Oficina de Planeación y Oficina de Sistemas
Daño informático		
Riesgos organizativos internos o externos	Mapa de Riesgos	Oficina de Planeación
De corrupción	Mapa de Riesgos de Corrupción (Estrategia Anticorrupción y de Atención al Ciudadano)	Oficina de Planeación

Se debe considerar que se contemplen las acciones a realizar en relación con los recursos propios involucrados en procesos críticos, y que se consideren los riesgos y soluciones del ambiente social, físico y de seguridad, relacionados con la operación de los procesos principales de la Entidad. Las actividades y procedimientos, están relacionados con las funciones que competen a cada uno de los grupos contingentes establecidos para la ejecución del PCL y dependen de



la diligencia y colaboración de las dependencias internas y de los recursos disponibles (presupuesto, capacitación, recursos técnicos, etc.)

#### **1.4. ORGANIZACIÓN INSTITUCIONAL PARA LA ADMINISTRACIÓN DE RIESGOS Y CONTIGENCIAS**

La siguiente es la estructura y funciones que se define para la administración del riesgo, sin perjuicio de la actividad que cada dependencia debe cumplir para ello.

##### **1.4.1 Comité Directivo**

Conformado por funcionarios del nivel directivo y ejecutivo de la Procuraduría General de la Nación:

- Viceprocurador (a) General
- Director del Instituto de Estudios del Ministerio Público
- Delegada para Asuntos Ambientales y Agrarios
- Secretario(a) General
- Jefe Oficina de Planeación
- Jefe Oficina de Control Interno
- Jefe Oficina de Sistemas
- Jefe División de Seguridad
- Jefe División Administrativa
- Jefe Oficina de Prensa
- Coordinador Grupo Bienestar Social Integral

La coordinación y dirección del Comité estará precedido en todo momento por el Viceprocurador (a) General de la Nación.

El Comité Directivo tendrá las siguientes funciones antes, durante y después de activada la emergencia en la Entidad:

**Definir** los lineamientos de los planes, manuales y guías para Contingencias en la Procuraduría General de la Nación a Nivel Nacional.

**Orientar, evaluar y controlar** el desarrollo e implantación de los mismos.

**Estudiar, evaluar y decidir** sobre los requerimientos que se presenten en el desarrollo e implantación de los planes y programas de prevención.



**Recomendar** acerca de la asignación de recursos o la adquisición y el mantenimiento de equipos, programas e instalaciones.

**Definir, asignar funciones y estructurar** los grupos de desarrollo para la implantación, mantenimiento, seguimiento y control de **PCL**.

**Estudiar, evaluar y decidir** sobre los requerimientos, ajustes o recomendaciones planteadas por los grupos.

**Resolución Número 256 del 15 de septiembre de 2006 “Por medio de la cual se adopta el Plan de Manejo de los Riesgos Institucionales”**

*“ARTICULO 2. - Para la administración del riesgo a nivel institucional se establecen las siguientes obligaciones:*

*a) El nivel directivo, con el apoyo de la Oficina de Planeación, establecerá las políticas para el manejo de todos aquellos eventos que puedan afectar negativamente el logro de los objetivos y metas institucionales.*

*b) Los Procuradores Delegados, Auxiliares, Regionales, Provinciales y Judiciales, el Secretario General y los Jefes de Oficina y de División, serán responsables de mantener actualizados los Mapas de Riesgos de sus dependencias, y de implementar las técnicas, procedimientos y controles para garantizar que la respuesta a los riesgos identificados se lleven a cabo adecuada y oportunamente; actividades que deben ser plasmadas en sus planes operativos anuales -POAS- .*

*c) La Oficina de Planeación, será la encargada de diseñar, administrar y mantener actualizado el Plan de Contingencias Logísticas, en el cual se señalan las políticas institucionales referidas a la administración de riesgo, así como las medidas específicas para actuar frente a aquellos riesgos residuales no asegurables, identificados por las dependencias, descritos, analizados y calificados en el Mapa de Riesgos institucional.*

*d) La Oficina de Control Interno, hará seguimiento a las acciones que se desarrollen para una efectiva administración del riesgo y realizará el monitoreo al Plan de Contingencias Logísticas, a fin de sugerir los correctivos y ajustes necesarios para asegurar que el manejo del riesgo residual se esté llevando a cabo de manera eficaz.*



*e) Los servidores, aplicarán los lineamientos establecidos para la administración del riesgo y participarán activamente para la aprehensión de las nuevas prácticas propuestas, que exigen valores y principios éticos, el ejercicio del auto-control y la auto-evaluación, calidad en la información generada y compartida, decisiones oportunas y eficaces, así como la racionalidad en la utilización de los recursos institucionales”.*

#### **1.4.2 Coordinadores de los planes y programas de contingencias**

Los Coordinadores son responsables en la Entidad, del tema de prevención y atención que les sea asignado y a través de ellos, se transmitirán las decisiones tomadas.

Así mismo, deben encargarse de monitorear y asegurar el cumplimiento del Plan, Programa, Manual o Guía y del mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo, proveer los recursos necesarios y notificar las decisiones a los funcionarios delegados. En su ausencia podrán delegar a funcionarios asignados a sus dependencias o de los grupos definidos por el Comité Directivo.

#### **1.4.3 Grupos de desarrollo de los planes de emergencia y contingencia**

Son conformados por servidores de la PGN, responsables de la ejecución de las acciones de prevención o atención, definidas dentro de los planes, programas y manuales; su conformación y funcionamiento será propuesta por el Coordinador temático y aprobada por el Comité Directivo. Cada grupo contará con su programa de trabajo, así mismo se conformarán los siguientes equipos para la ejecución de planes, que igualmente serán propuestos por el Coordinador y aprobados por el Comité Directivo

Los grupos de desarrollo tendrán las siguientes funciones antes, durante y después de activada la emergencia en la Entidad:

- Ejecutar cada una de las actividades planeadas.
- Documentar y formalizar planes, programas y manuales de contingencias.
- Diseñar planes de entrenamiento para los funcionarios de la entidad, a todo nivel, para que estén en condiciones de evitar o atender contingencias.



- Diseñar cronogramas y apoyar logísticamente las pruebas de cada segmento del plan.
- Mantener operativos y actualizados los planes, programas o manuales de contingencias.

#### **1.4.3.1 Equipo de Atención de Emergencias.**

Este grupo se encargará de activar las medidas necesarias para salvaguardar los recursos humanos y materiales.

#### **1.4.3.2 Equipo de Evaluación de Daños.**

Se encargarán de la revisión del talento humano, la planta física, identificando los daños físicos y lógicos (Hardware y Software) originados durante la contingencia, informando los resultados al Comité Directivo

#### **1.4.3.3 Equipo de Seguimiento y Control.**

Conformado por los funcionarios de las Oficinas de Planeación, Control Interno, Sistemas y del Grupo de Bienestar social Integral, apoyados por el funcionario coordinador de las labores del área; quienes se encargaran de hacer seguimiento y control a las labores que se ejecuten, velando por el respectivo plan y la seguridad en su efectiva aplicación, así como la coherencia y consistencia en la aplicación de los procedimientos establecidos.



## 1.5 PROCESO GENERAL DE CONTINGENCIA

Como proceso general se consideran las siguientes etapas: antes, durante y después de que se presente una contingencia:

Planear	ANTES	Identificar riesgos, definir procesos, estructura, funciones, roles, documentos de referencia y recursos.
Organizar		Elaborar manuales, procesos y protocolos planeados.
Institucionalizar		Aprobar planes, programas y manuales y ponerlos en funcionamiento.
Prevenir	DURANTE	Desarrollar las acciones de capacitación y comunicación para evitar la ocurrencia de un siniestro o concreción de un riesgo, así como tomar las medidas necesarias para reducir la probabilidad de ocurrencia
Atender		Cumplir los protocolos previstos ante una situación de emergencia o contingencia.
Restaurar	DESPUÉS	Adelantar las acciones necesarias para que el funcionamiento institucional retorne a la normalidad.
Evaluar		Valorar situaciones vividas y los niveles de exposición al riesgo, para definir acciones que generen el aprendizaje organizacional.



### 1.5.1 SIMULACROS

Los planes de contingencias de la PGN deben considerar simulacros de diferentes siniestros y situaciones para comprobar que la organización y sus protocolos sean eficaces y oportunos.

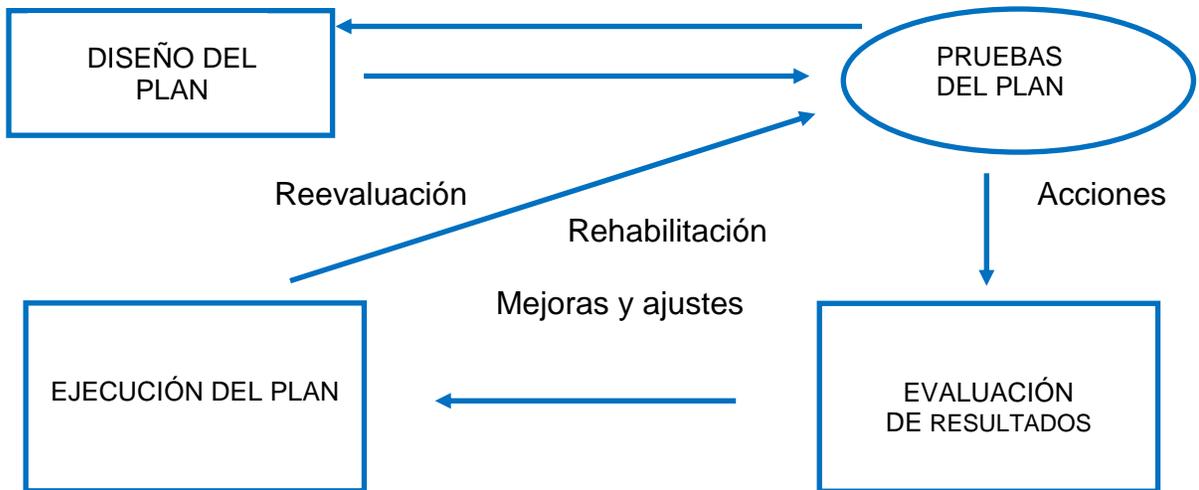
Los pasos de los procedimientos definidos para la realización de las pruebas programadas en la fase de diseño, ejecución, seguimiento y control se muestran en la gráfica 1.

Los siguientes son los objetivos de control y seguimiento de las pruebas del plan:

- **Validar** la habilidad de los funcionarios y la consistencia de los procedimientos en eventos de recuperación de siniestros.
- **Probar** la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- **Identificar y corregir** fallas.
- **Facilitar** la divulgación y el entrenamiento en los procedimientos y guías de recuperación.
- **Fomentar** el respectivo plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias.
- **Evaluar** las necesidades de seguros y reducir al máximo los costos en primas de aseguramiento.
- **Motivar** a los funcionarios involucrados en el diseño y desarrollo del plan, a mantener actualizados los procedimientos inherentes.

Gráfica 1. Fases de los procedimientos de pruebas del plan.

**MEDIDAS PREVENTIVAS PLAN DE ACCIÓN**





## CAPÍTULO II. MARCO TEÓRICO

Al interior de la PGN existe una gama diversa de planes y programas para anticiparse y definir los propósitos a alcanzar. Con el fin de unificar el lenguaje, se considera en principio que existen tres tipos de actividades de planeación:

Tipo de planeación	Temática	Propósito
Planeación Estratégica	Factores críticos de éxito globales	Desarrollar la PGN
Planeación Operativa	Día a día: operación, procesos, programación de recursos y actividades	Gestionar la operación hacia objetivos
Planeación Contingente	Riesgos y Emergencias	Reducir la vulnerabilidad a riesgos y aumentar la preparación para su atención

La Oficina de Planeación formula y elabora el PCL para la Procuraduría General de la Nación, proceso que se inicia solicitando a las dependencias del nivel directivo, asesor y ejecutivo del Orden Central y Territorial, la relación de riesgos con probabilidad de ocurrencia real y que generen un impacto negativo o interrupción parcial o total, en el cumplimiento de las Funciones Misionales o de Apoyo Administrativo encomendadas a la Institución. A partir de ellas se lista los diferentes riesgos de origen:

- **Natural:** inundaciones, terremotos, maremotos, erupciones volcánicas, avalanchas, tornados, huracanes, ciclones, tormentas eléctricas, etc.
- **Tecnológico:** explosiones, derrame de productos químicos, liberación de sustancias tóxicas, intoxicaciones, colapso de edificaciones, fallas estructurales, exposición a radiaciones ionizantes, falta de servicios públicos, daños a máquinas y equipos.
- **Social:** Derivado de conflictos sociales, guerras, desórdenes civiles, protestas urbanas, atentados, terrorismo, etc.

Estos riesgos pueden tener una posibilidad de ocurrencia mayor o menor de acuerdo a los procedimientos de seguridad establecidos y que correspondan a estrategias concretas definidas y adoptadas por la PGN para mitigar el impacto negativo de los mismos.



En ese orden de ideas y sabiendo que el recurso más valioso de la Entidad es el talento humano y que para mitigar un posible daño grave o leve al mismo, se hace necesario atenuarlo mediante la redistribución óptima de los recursos físicos, tecnológicos, financieros y de la memoria institucional que permita a la Procuraduría continuar cumpliendo la misión asignada por ley, la cual requiere mantener operando y desarrollando los procedimientos administrativos.

Es fundamental realizar tareas tales como:

- **Calcular** el tiempo durante el cual la Entidad puede funcionar sin sedes, con disminución dramática de personal, sin servicios públicos, sin recursos informáticos en operación o sin memoria documental.
- **Reconocer y detallar** las amenazas potenciales sobre la capacidad de ejecución de los procesos institucionales, infraestructura, tecnología y talento humano.
- **Definir** las aplicaciones críticas que deben ser procesadas mientras se restablecen las operaciones normales en la Entidad.
- **Determinar** las consecuencias operativas, estratégicas y/o legales, por la carencia del servicio institucional.
- **Establecer y valorar** la inversión en el desarrollo del PCL, que asegure la continuidad y normal funcionamiento de la Entidad.

En consideración a lo expuesto, se proponen como Fases de Evaluación y Seguimiento, las siguientes:

- **Fase de Mitigación:** aseguramiento y conservación del talento humano, infraestructura física, maquinaria y equipo, memoria institucional y la continuidad en la ejecución de procesos y procedimientos, que incluyen la atención a clientes internos o externos, el procesamiento de datos, aplicaciones automáticas críticas, en caso de falla de su Software o Hardware.
- **Fase de Emergencia:** contiene las acciones detalladas que deben ser llevadas a cabo durante el siniestro o emergencia causada por la activación real del riesgo previamente señalado.



- **Fase de Recuperación:** permite restablecer las condiciones originales y operación normal de los procedimientos institucionales de la dependencia o sede afectada y superar las dificultades que impiden prestar sus servicios a la sociedad.

Aplicadas de manera coherente y segura las fases anteriores se debe continuar con la ejecución o desarrollo de los siguientes procedimientos:

- **Revisión:** comprende la determinación de vulnerabilidad del área, inventario de recursos y limitaciones que se presentan en la misma.
- **Evaluación del Impacto por Interrupción del Servicio:** comprende la estimación de las pérdidas asociadas a vidas humanas, información, documentos, infraestructura física, maquinaria y equipo que no permitan ejecutar los procedimientos misionales y administrativos asignados por la ley y que generan suspensión parcial o total de actividades.

Esta evaluación se da en términos de las consecuencias que originaría dicha suspensión de acuerdo al análisis de riesgos

- **Implementación:** se realizan actividades específicas para la reducción y eliminación de riesgos, que proponen las medidas de acción, en caso de presentarse alguna situación de emergencia.
- **Cronograma:** el diseño de un cronograma de trabajo, provee la oportunidad de registrar los logros de cada tarea, verificar si en realidad las actividades han sido cumplidas o no en el tiempo previsto y analizar cuáles han sido los principales inconvenientes que se han presentado si se detectan desviaciones importantes en el cronograma inicial, antes de la ejecución de las pruebas.
- **Documentación:** se prepararán y archivarán todos los documentos donde se registren las actividades, logros e inconvenientes, programas, objetivos, cronograma, procedimientos, planillas y casos fundamentales referentes a las acciones generadas durante el desarrollo del PCL de la Procuraduría General a Nivel Nacional, quedando con ello un historial documental de referencia.
- **Simulación o simulacro:** se define el alcance y el cronograma de simulacros, así como se designa a los responsables de dar inicio a las pruebas, ambientar el personal y los recursos, controlar los eventos, documentar las acciones y evaluar el resultado en su conjunto.



- **Ejecución:** actividades propuestas para ejecutar, tienen que ver con el desarrollo de Medidas de protección planificadas por cada dependencia o sede afectada:
  - 1) Iniciación de las acciones destinadas, por prioridad, a controlar la situación durante los primeros instantes de la emergencia.
  - 2) Consideración de las responsabilidades extraordinarias que el comité directivo del plan tendría que asumir, a fin de ofrecer protección y seguridad al talento humano, instalaciones, memoria institucional y equipos y sistemas de información del área, dependencia o sede afectada.
  - 3) Evaluación del ejercicio, considerando como elemento vital al recurso humano, luego a las instalaciones y equipos y sistemas de información, con los cuales se garantiza la operación de los procedimientos planificados para la recuperación total del servicio.

El **PCL** de la Procuraduría se convierte en la Guía Institucional de prevención, atención y administración de riesgos, para:

- **Establecimiento** de procedimientos contingentes, organización de grupos de trabajo, funciones y responsabilidades, involucrando funcionarios de todos los niveles jerárquicos en cada dependencia o sede de la Entidad.
- **Adopción formal** de un grupo para administrar las emergencias, con mecanismos de notificación claramente establecidos.
- **Definición de escenarios** para modelar riesgos asociados a la planta, los procedimientos, documentos, sistemas de información e infraestructura.
- **Diseños de programas** de almacenamiento y estrategias.
- **Detalle** de la administración general del Plan.

## 2.1. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

El análisis de riesgos implica la evaluación del impacto por interrupción de la prestación de servicios a los clientes externos o internos, el cual comprende la estimación de las pérdidas que involucraría la suspensión parcial o total del



funcionamiento; esta valoración se da en términos de las consecuencias que acarrearía dicha suspensión.

En esta etapa se desarrolla la probabilidad de ocurrencia, grado de preparación (capacidad de mitigación y reducción de impacto de los riesgos), finalmente las alternativas de corrección de la anomalía presentada. Los riesgos potenciales que pueden afectar la continuidad y operatividad normal.

### 2.1.1. Riesgos externos

- **Posibles fallas en el Flujo de Energía Eléctrica:** este riesgo está relacionado con amenazas externas al control de la Entidad. Sin embargo, se han adquirido equipos para mitigar el riesgo de corte temporal de Energía Eléctrica, dado que la Procuraduría tiene: UPS (unidad de poder ininterrumpido) en cada una de las redes de área local y LAN para salvaguardar la información durante aproximadamente una (1) hora. Si el corte es más prolongado.
- **Mantenimiento:** Este depende de la empresa prestadora del servicio en cuanto a la estructura, grupo de inmuebles en cuanto a las redes internas, y la oficina de sistemas para las UPS.
- **Torres A y B:** Planta eléctrica propiedad de la PGN y su control, mantenimiento y funcionalidad depende de la misma, en caso de falla en el suministro tiene capacidad para abastecer el funcionamiento de 2 ascensores (carro I y carga), Centro de Computo, UPS de 80 Kw., 1 aire de precisión del Centro de Computo y Sala Técnica de la División de Seguridad, áreas comunes y las escaleras internas, estas a su vez, disponen de lámparas de emergencia. Se están instalando lámparas de emergencia en pisos y en la actualidad se disponen en 2º, 4, auditorio, 6, 16, 19, 20, 25, 28.

Es indispensable nombrar que en la actualidad no existe un contrato para el mantenimiento de las plantas de las torres correspondiente.

- **Recomendación:** Realizar un contrato con la empresa prestadora del servicio para realizar mantenimiento a las estructuras de la PGN.
- **Torre C:** Planta eléctrica propiedad de la PGN y su control, mantenimiento y funcionalidad depende de la misma, esta planta posee la capacidad de suministrar el servicio en todo el edificio; se ha realizado gestiones de



mejora en el suministro de energía, mediante un cambio de transformador lo que conlleva a que mejore esta tanto en las protecciones medias como altas.

El contrato de mantenimiento de la presente, está cumpliendo actualmente con la garantía correspondiente.

- **Ed. Manuel Mejía:** 1 Planta propiedad de la copropiedad horizontal.
- En **Arauca, Montería, San José del Guaviare, Mitú y Riohacha** se cuenta con una pequeña planta de combustible. El problema en las Regionales es que las plantas son pequeñas y conectan los aires acondicionados y no son suficientes para abastecer estas necesidades.
- **Fallas en el servicio de Acueducto.** Aunque este riesgo presente amenazas a la Entidad, la Administración del Edificio, posee 2 motobombas de agua potable en el sótano del edificio, que impulsan hasta la azotea del edificio distribuyéndolo por cada piso, realizando mantenimiento correctivo integral tanto a los motores, las bombas y los tableros o sea a todo el sistema incluidas (válvulas, cheques y tanques), también posee una bomba de drenaje en el tercer sótano.
- **Torres A y B:** 6 Tanques de agua de 25mt/3 en el sótano y 1 de 27 MT/3 en la azotea, en caso de corte del suministro abastecen por 4 a 6 horas dependiendo del No de personas, el mantenimiento que se le realiza a estos tanques, es correctivo.
- **Torre C:** 6 tanques de agua de 1000 ATS que funcionan por gravedad.
- **Ed. Manuel Mejía:** Cuenta con dos tanques de reserva, ubicados en el sótano y la terraza del edificio.
- **Mantenimiento:** Cuenta con dos tanques de reserva, ubicados en el sótano y la terraza del edificio, y dependen de la administración.
- **Posibles fallas del Servicio Telefónico:** Evitando la amenaza externa de la suspensión de este servicio la procuraduría puede efectuar una debida mitigación mediante el uso de comunicación vía canales dedicados, una situación que se presento fue la ampliación de los teléfonos IP (extensiones) presentándose una saturación que se corrigió o se subsano este riesgo para beneficio de la Entidad, en cuanto al servicio de la



conectividad está garantizada entre las Regionales y el nivel central, lo mismo que el acceso internet.

- La PGN dispone de Telefonía - IP. - tradicional e híbrida. El servicio de telefonía depende del operador local que suministre el servicio dependiendo del territorio donde se encuentre, en el caso de Bogotá actualmente, la empresa prestadora del servicio es TELEFÓNICA / TELECOM y el servicio debe ser restablecido máximo en 8 horas.
- **Mantenimiento:** Este le corresponde a tres; La empresa prestadora del servicio, es decir el operador, la Supervisión de servicios públicos y tercero la dependencia de sistemas.
- **Posibles fallas o desabastecimiento de Suministros de Oficina:** Este riesgo está relacionado con amenazas externas al control de la Entidad, como lo es el desabastecimiento de Suministros de Oficina, mayor a un día laboral y la Procuraduría no puede efectuar una debida mitigación. Aunque existen amenazas de riesgos externos la Jefatura del Almacén ha diseñado una política de tener un stop de suministros en bodega, suficientes para suplir los requerimientos de las distintas dependencias a nivel central y poder abastecer de suministros a todas las oficinas.

### 2.1.2. Riesgos internos

- **Perdida de Información y Daño de Documentos en el Archivo Central y de Gestión:** se asocia a pérdidas originadas por la sustracción o deterioro de documentos por agua, hongos, bajas o altas temperaturas, químicos, líquidos, humos, gases y vapores, manejo de herramientas, proyección de partículas, manipulación de maquinaria. Se presenta un riesgo alto por cuanto al archivo se encuentra en un lugar que no es apropiado, saturado por espacio físico, en la actualidad se encuentran realizando el traslado hacia la nueva sede de Archivo, la cual se ubicada en el barrio Samper Mendoza en la ciudad de Bogotá, dando así solución a los problemas que se presentan, a nivel regional se presentan riesgos que requieren de soluciones por parte de la División Administrativa, dado lo específico de cada una de las sedes, por lo cual se recomienda que este sea subsanado o aminorado.
- **Recomendación:** Cada Regional debe tener la autonomía de contar con espacios adecuados para su archivo, y esta a su vez ser supervisada por la persona competente jerárquicamente, y vigilada por la dependencia que haga sus veces.



- **Errores y demoras institucionales** asociadas a Agentes y Factores de Riesgos de Origen Tecnológico como:
  - Físicos: ruidos, inadecuada iluminación, bajas o altas temperaturas.
  - Químicos: sólidos, líquidos, rocíos, neblinas, humos, gases y vapores.
  - Mecánicos: manejo de herramientas, proyección de partículas, manipulación de maquinaria, eléctrica y electrónica.
- **Demoras en la aplicación del PCL e incumplimiento de sus objetivos:** este riesgo tiene una alta probabilidad de ocurrencia por los escasos recursos para la ejecución de proyectos de prevención, de talento humano, de infraestructura, de procedimientos y de tecnología que implican grandes inversiones; lo que generaría incumplimiento de los cronogramas de ejecución y objetivos planteados en los proyectos referidos al cumplimiento misional, documental, sistematización y de gestión entre otros.
- **Posible mal funcionamiento del SOFTWARE y HARDWARE** como los cálculos que se realizan en programas de base de datos, contabilidad, nómina, hojas de cálculo, programas de mantenimiento y en sistemas de seguridad, que pueden presentar bloqueos o interrupciones que impidan el desarrollo normal de las funciones institucionales, como es acceso a la información contenida en la página WEB de la PGN, acceso directo al hosting de contingencia a través de la dirección IP, en el sistema de información Data Center. Es importante resaltar que dentro de los sistemas de información, se maneja los sistemas misionales, disciplinarios y los antecedentes, lo cual fue un desarrollo institucional por parte de la PGN.
- **Posible pérdida de información:** este riesgo tiene baja probabilidad de ocurrencia, teniendo en cuenta que el PCL incluye un proceso de respaldo, que permite la mitigación del riesgo, efectuando copias de respaldo (Backups), tanto a los archivos de trabajo (Word, Excel, PowerPoint, otros ), como a los archivos de base de datos y resultados de las aplicaciones específicas ( información contenida en servidores de base de datos, servidores Web, servidores de Red, equipos de comunicaciones, Librería de Backups y File Server, etc.) en producción para cada una de las dependencias y archivo documental de los Procesos Misionales a Nivel Nacional, debido a que la Entidad ha implementado procedimientos para su mitigación, tales como:

La instalación en el centro de un nuevo data center de refrigeración, además se cuenta con cómputo principal (piso 5º) de un sistema de temperatura autorregulada, provisto de un sistema de aire acondicionado, con sensores



ambientales para el control y monitoreo de temperatura, humedad, flujos de corriente, filtros de aire, alarma local y silenciosa. Este sistema se encuentra conectado con la cámara principal a través de conductos para el control de los flujos de corriente y aire, y en el techo está provisto de detectores de humo y fuego que accionan un sistema de alarmas y descarga automática de gases que apagan llamas originadas en el salón de la UPS y Servidores de la Red, bajando así la probabilidad de ocurrencia.

- **Riesgos internos asociados al Centro de Cómputo Principal:** un análisis del medio y los procedimientos de seguridad y control existentes indica que la Entidad está en una posición favorable por lo siguiente:
  - El Edificio no se encuentra en una zona que pueda presentar inundación.
  - Se realizó un cambio de ubicación del centro de cómputo, en el piso 2 de la torre C, ubicado estratégicamente en el Edificio de la sede central en Bogotá, posee detectores de humo y fuego que accionan un sistema de alarmas y de descarga automática de gases que apagan las llamas originadas en el salón de la UPS y cuarto de servidores, y está provisto de una temperatura autorregulada.
  - El centro de cómputo ubicado en el 5 piso de la torre A, está pendiente para trasladar los equipos en el centro nuevo de cómputo de la torre C.

En el mismo análisis del medio y procedimientos de seguridad y control se detectó que la Procuraduría presenta algunas limitaciones como las siguientes:

- El Centro de Cómputo de la Entidad **no** dispone de un piso falso, con el cual se podría dar aislamiento de cargas estáticas.
- La Entidad **no** cuenta con una solución robótica para la generación automática de copia de respaldo de la información (backups).



## **CAPÍTULO III. SUSPENSIÓN DE SERVICIOS PÚBLICOS**

### **3.1. Definición**

Es la disminución o corte que se presenta en el suministro de uno de los siguientes servicios públicos: Agua, Energía, Teléfono y Recolección de Basuras.

### **3.2. Procedimiento**

Los siguientes son los protocolos a seguir en caso de que ocurra la situación.

### **3.3. Procedimiento en caso de suspensión de agua, energía y teléfono o recolección de basuras**

Actividades:

- Corresponde al Coordinador del Grupo de Inmuebles velar porque existan plantas eléctricas en las distintas sedes de la PGN, tanto a nivel central como territorial y que estén en condiciones de operar. En caso que este servicio no se este prestando, corresponde al Secretario General definir la sedes que contarán con estos equipos y servicios e impulsar la adquisición de los mismos, conforme a las disponibilidades presupuestales existentes.
- En las sedes que cuenten con plantas eléctricas, estas deben incluir un sistema que les permita encenderse de forma automática en caso de corte en el suministro de Energía Eléctrica.

#### **Sedes del Nivel Central**

Actividades:

- 1) El Jefe de la División Administrativa se reúne con el Administrador del Edificio o quien haga sus veces (el Coordinador del Grupo de Inmuebles), Oficina de Sistemas y División de Seguridad, para determinar: período de suspensión, causas de la suspensión y acciones definidas por la Empresa de Acueducto o Empresa de Energía o Empresa de Teléfono o de Recolección de Basuras.
- 2) El Jefe de la División Administrativa, con los servidores precitados determina cambios en la jornada laboral y medidas como: cierre de los servicios sanitarios, abastecimiento a través de carro tanques, soporte con plantas



eléctricas, abastecimiento de combustible para las plantas, suspensión del servicio, desconexión de los equipos de las redes eléctricas, otras; en caso de los teléfonos servicios sustitutos como : telefonía celular, correo electrónico, mensajería, atención personalizada y en caso de la Recolección de Basuras, recolección a través de Empresas Nacionales o Distritales de Obras Públicas u otros cambios en la jornada laboral.

- 3) Se informa al Secretario General la situación y se le solicita autorización para el desarrollo de las actividades que así lo ameriten.
- 4) Se informa al Procurador General de la Nación sobre la situación y se solicita autorización para el desarrollo de las actividades que así lo requieran.
- 5) Se comunica a nivel institucional la duración de la suspensión y las medidas a tomar.
- 6) La Oficina de Prensa comunica a la ciudadanía, las situaciones que afecten el normal funcionamiento de los servicios institucionales.
- 7) Superada la situación el Jefe de la División Administrativa se encargará de coordinar las actividades necesarias para el restablecimiento de los servicios internos, tales como: cafetería, sanitarios, el estado de la red y del fluido eléctrico e informar sobre la reconexión de los equipos a las redes eléctricas, teléfonos y verificar la situación sanitaria de los Depósitos de Basuras con el fin de evitar problemas de salud en los funcionarios.
- 8) El Jefe de la División Administrativa presentará un informe al Secretario General sobre los hechos que generaron la situación y la forma como la Entidad afrontó la misma en procura de mejorar la respuesta y preparación institucional.

### **Sedes del Nivel Territorial**

Actividades:

El Procurador Regional asume el desarrollo de las acciones definidas que sean de su competencia.

- 1) Se reúne con el Coordinador Administrativo y se comunica con la Oficina de Sistemas del Nivel Central para determinar: período de suspensión, causas de la suspensión, acciones definidas por la Empresa de Acueducto o Empresa de Energía o Empresa de Teléfonos o Empresa de Recolección de Basuras.



- 2) Se reúne con el Coordinador Administrativo evalúan las medidas a tomar, como: cierre de los servicios sanitarios, abastecimiento a través de carro tanques, soporte con plantas eléctricas, abastecimiento de combustible para las plantas, cambios en la jornada laboral, suspensión del servicio e informan sobre la desconexión de los equipos de las redes eléctricas, evalúan en la suspensión del servicio telefónico medidas como: telefonía celular, correo electrónico, mensajería, atención personalizada; recolección de basuras a través de Empresas Municipales o Distritales de Obras Públicas u otros, y comunican a nivel regional la duración de la suspensión y las acciones a seguir, y a la ciudadanía las situaciones que afecten el normal funcionamiento de los servicios institucionales.
- 3) Superada la situación se encarga de coordinar las acciones necesarias para el restablecimiento de los servicios internos tales como: cafetería, sanitarios, verificar el estado de las redes, del fluido eléctrico e informan la reconexión de los equipos a las redes eléctricas y verifican la situación sanitaria de los Depósitos de Basuras y demás.
- 4) Presenta un informe al Secretario General sobre los hechos que generaron la situación y la forma como la Procuraduría Regional afrontó la misma en procura de mejorar la respuesta y preparación institucional.

#### **3.4. SUSPENSIÓN POR INCUMPLIMIENTO EN LOS PAGOS A LOS PRESTADORES DE SERVICIOS**

Cuando la suspensión se origina en el incumplimiento en el pago de los servicios, se procede así:

Una vez conocida la situación el Jefe de la División Administrativa deberá en forma inmediata comunicar al Jefe de la División Financiera.

- 1) El Jefe de la División Financiera establecerá las causas del no pago y evaluará alternativas de actuación tales como: requerimientos al Ministerio de Hacienda, solicitudes a empresa prestadora del servicio para su reconexión, abonos a las deudas existentes.
- 2) El Jefe de la División Financiera informa al Secretario General la situación y las medidas que se pueden tomar.
- 3) El Secretario General evalúa con el Jefe de la División Administrativa y el Jefe de la División Financiera las acciones a desarrollar.



- 4) El Secretario General autoriza u obtiene la autorización respectiva del Procurador General, en caso de ser necesario, para el desarrollo de las acciones.
- 5) El Jefe de la División Financiera asume el desarrollo de las acciones definidas que sean de su competencia.
- 6) El Jefe de la División Financiera presenta un informe al Secretario General sobre los hechos que generaron la situación y la forma como la Procuraduría Regional afrontó la misma en procura de mejorar la respuesta y preparación institucional.

**Responsables :**

Secretaria General  
Procuradores Regionales  
Jefe Oficina de Prensa  
Jefe División Administrativa  
Jefe División Financiera  
Jefe de Dependencia o Unidad del Nivel Territorial  
Coordinador Grupo de Bienes Inmuebles  
Coordinador Grupo de Muebles y Servicios Administrativos  
Coordinadores Administrativos



## **CAPÍTULO IV. DESABASTECIMIENTO DE SUMINISTRO DE ELEMENTOS DE OFICINA Y DE TRABAJO**

### **4.1. Definición**

Es la disminución o corte que se presenta en la entrega de dotación de insumos y elementos necesarios de trabajo, tales como: papelería, tintas, toner, disquetes, gasolina, repuestos y demás, sin los cuales se afecta la prestación de los servicios institucionales.

### **4.2. Procedimientos**

Cuando el desabastecimiento se origine en el incumplimiento en el pago de los contratos u ordenes de suministro que generan la orden de suspensión por parte del proveedor, se procede así:

- 1) Una vez conocida la situación el Jefe de la División Administrativa deberá en forma inmediata, comunicar al Jefe de la División Financiera.
- 2) El Jefe de la División Financiera conjuntamente con el Jefe de la División Administrativa, establecerán las causas del no pago y evaluarán alternativas de actuación tales como: requerimientos al Ministerio de Hacienda, acuerdos de pago, mediante abono, a la empresa contratada para la normalización del suministro.
- 3) Los Jefes de División precitados, informan al Secretario General la situación y las medidas que se pueden tomar.
- 4) El Secretario General evalúa con los Jefes de División citados, las acciones a desarrollar.
- 5) El Secretario General autoriza u obtiene la autorización respectiva, del Procurador General en caso de ser necesario, para el desarrollo de las acciones.
- 6) El Jefe de la División Financiera y el Jefe de la División Administrativa asumen el desarrollo de las acciones definidas que sean de su competencia.
- 7) El Jefe de la División Administrativa presentará un informe al Secretario General sobre los hechos que generaron la situación y la forma como la



Procuraduría Regional afrontó la misma en procura de mejorar la respuesta y preparación institucional.

Cuando el desabastecimiento se origine en una situación de mercado, por inexistencia del bien, insuficiente importación, acaparamiento, situaciones sindicales de oferentes, o por cualquier otra causa (deficiencia presupuestal, robo etc.,) se procede así:

- 1) Una vez conocida la situación el Jefe de la División Administrativa deberá en forma inmediata comunicar al Secretario General.
- 2) El Jefe de la División Administrativa establecerá las causas y evaluará alternativas de actuación tales como: permuta con otras entidades del Estado, adquisición de bienes sustitutos, compra de bienes con proveedores internacionales.
- 3) El Secretario General evalúa con las personas pertinentes, según el bien, las acciones a desarrollar.
- 4) El Secretario General en caso de ser necesario autoriza, u obtiene la autorización respectiva de la Junta de Licitaciones y Adquisiciones para el desarrollo de las acciones.
- 5) El Jefe de la División Administrativa asume el desarrollo de las acciones definidas que sean de su competencia.
- 6) El Jefe de la División Administrativa presenta un informe al Secretario General sobre los hechos que generaron la situación y la forma como la procuraduría regional afrontó la misma en procura de mejorar la respuesta y preparación institucional.

**Responsables:**

Secretaria General  
Procuradores Regionales  
Coordinadores Administrativos  
Coordinador del Grupo de Bienes Inmuebles  
Coordinador del Grupo de Muebles y Servicios Administrativos  
Jefe de Dependencia o unidad del Nivel Territorial  
Jefe División Financiera  
Jefe División Administrativa  
Junta de Licitaciones y Adquisiciones



## **CAPÍTULO V. DAÑO MEMORIA INSTITUCIONAL - ARCHIVO**

### **5.1. Definición**

Un posible siniestro, como: incendio, inundación, contaminación o mutilación de la información que esta archivada en el Archivo Central de la PGN.

### **5.2. Procedimientos**

Corresponde al Coordinador del Grupo de Archivo Central velar porque en todo momento en el área de Archivo General se cumplan con los planes de mantenimiento locativo, sistemas de seguridad, servicio de aseo, niveles de temperatura y luz adecuados para que el Archivo Central, esté en condiciones de operar.

#### **Sedes del Nivel Central**

Actividades:

- 1) El Jefe de la División Administrativa se reúne con el Coordinador del Grupo de Inmuebles y el Coordinador del Grupo de Archivo Central para determinar: periodos de inspección, causas de deterioro documental, acciones definidas por prevención.
- 2) El Secretario General se reúne con los servidores precitados para determinar las medidas a tomar tales como: soporte con sistema alerno de conservación (microfilmación, disco óptico y/o copias adicionales), cambios en la jornada laboral, suspensión del servicio.
- 3) Se comunica a nivel institucional la duración de la suspensión y las medidas a tomar.
- 4) La Oficina de Prensa comunica a la ciudadanía las situaciones que afecten el normal funcionamiento de los servicios institucionales.
- 5) El Coordinador del Archivo Central en conjunto con el Jefe de la División de documentación elabora informe sobre la situación presentada y la forma como



se afrontó la misma en procura de mejorar la respuesta y preparación institucional.

### **Sedes de Nivel Territorial**

#### Actividades

- 1) El Procurador Regional se reúne con el Coordinador Administrativo y realizan las acciones para determinar: período de suspensión, causas de la suspensión, acciones definidas, comunica a nivel regional la duración de la suspensión y las medidas a tomar, comunica a la ciudadanía las situaciones que afecten el normal funcionamiento de los servicios institucionales.
- 2) El Procurador Regional y el Coordinador Administrativo evalúan las medidas a tomar tales como: soporte con sistema alerno de conservación microfilmación, digitalización, disco óptico y/o copias adicionales), cambios en la jornada laboral, suspensión del servicio.
- 3) Se informa al Secretario General sobre la situación y las medidas a tomar.
- 4) El Secretario General autoriza u obtiene la autorización respectiva para el desarrollo de las acciones y las informa.
- 5) El Procurador Regional asume el desarrollo de las acciones definidas que sean de su competencia.
- 6) Superada la situación el Procurador Regional se encarga de coordinar el restablecimiento de los servicios internos.
- 7) El Procurador regional presenta un informe al secretario General sobre los hechos que generaron la situación y la forma como la Procuraduría regional afrontó la misma en procura de mejorar la respuesta y preparación institucional.

#### **Responsables:**

Comité de Archivo  
Jefe Oficina de Prensa  
Jefe División Administrativa  
Coordinador Grupo de Bienes Inmuebles  
Coordinador Grupo de Muebles y Servicios Administrativos  
Coordinador Grupo de Archivo



Jefe División de Documentación  
Procuradores Regionales  
Coordinadores Administrativos

### **5.3. Implantación de soluciones**

La Procuraduría siguiendo los parámetros prioritarios de las políticas aprobadas en el Comité de Contingencias Logísticas, debe adoptar los siguientes procedimientos:

Paso 1: Adquirir equipos detectores de humo y sistemas contra incendio, ante la posibilidad alta de conato de incendio, inundación, contaminación biológica, particularmente en el nivel Regional.

Paso 2: Adquirir, actualizar e instalar detectores de humo a nivel central.

Paso 3: Aislar las salas con puertas contrafuego de manera que si se presentará algún siniestro con ellas se pueda proteger la documentación de las diferentes salas.

Paso 4: Capacitar a todos los funcionarios de la Entidad en sistemas de información y prevención de suministros ya que el alto desconocimiento y falta de cultura archivística son los que nos llevan a tener un impacto alto en este tipo de siniestros.

Paso 5: Eliminar el polvo de documentos y estantes una vez por semana junto con la realización de inspecciones periódicas de las colecciones y locales una vez cada tres meses.

Paso 6: Programar fumigaciones contra las diferentes plagas y sebos con veneno.

Paso 7: Implementar la utilización de medios de protección para los funcionarios, tales como guantes, tapabocas, batas y mascararas si llegara el caso.



## CAPITULO VI. PLAN DE CONTINGENCIAS LOGÍSTICAS INFORMÁTICAS PCLI

### 6.1. Objetivos

- **MINIMIZAR** el tiempo de interrupción de las actividades realizadas en el Centro de Cómputo de la Oficina de Sistemas debido a la ocurrencia de una contingencia.
- **MANTENER LA CONTINUIDAD** del procesamiento de la información de la Entidad durante el tiempo que transcurra entre la ocurrencia de la contingencia y el restablecimiento y recuperación total de las condiciones normales de procesamiento.
- **DISMINUIR** impactos y minimizar los daños y las pérdidas económicas que pudieran derivarse.
- **INCREMENTAR** la capacidad de la Oficina de Sistemas para garantizar el almacenamiento y el procesamiento de la información procesada y generada en los equipos servidores del Centro de Cómputo, en condiciones ambientales y de seguridad adecuadas y dentro de niveles razonables de costo.
- **CONTROLAR Y ADMINISTRAR** el proceso de retorno a la normalidad y la restauración correcta de los servicios informáticos, luego de la ocurrencia de una contingencia.
- **MANTENER** la prestación y el soporte de los servicios de la red de comunicaciones de la Entidad ante la ocurrencia de una contingencia.

### 6.2. Alcance

El Plan tiene el siguiente alcance:

- Centro de Cómputo de la Oficina de Sistemas
- Infraestructura de Hardware, de Software base/productividad/aplicativo y de Servicios Informáticos, bajo la responsabilidad de la Oficina de Sistemas para su operación o soporte.



- El Plan está diseñado para enfrentar emergencias en la funcionalidad de la infraestructura informática, derivadas de la ocurrencia de contingencias y está dado por los siguientes aspectos:
- El análisis de los riesgos vinculados al Hardware y Software de procesamiento y comunicaciones, que por la presencia de las probables contingencias identificadas, interrumpen la continuidad y eficiencia de la Oficina de Sistemas, en la prestación de servicios informáticos y al apoyo que brinda a las operaciones misionales y administrativas de la Entidad.
- La definición de los procedimientos que determinan lo que se debe hacer en los casos de ocurrencia de cualquiera de las contingencias identificadas.

### 6.3. Fases del Plan

#### 6.3.1. Identificación de requerimientos

Tarea 1. Describir el ambiente organizacional y de proceso de la Oficina de Sistemas.

Tarea 2 Realizar el inventario general de los recursos y servicios informáticos internos (Equipos servidores de comunicaciones y estaciones de trabajo, computadores de escritorio, equipos electrónicos no informáticos, Software Base de procesamiento, etc.)

Tarea 3. Conformar los Equipos de Trabajo del Plan y asignar responsabilidades.

La función principal de los Equipos de Trabajo es ejecutar el **PCLI** ante situaciones de emergencia por la presencia de una contingencia que afecte la capacidad de la infraestructura informática para:

- **Mantener** operativas y funcionales tanto los Sistemas de Información Misionales y de Apoyo Administrativo de la Entidad como la prestación de los servicios informáticos por parte de la Oficina de Sistemas.
- **Restaurar** dentro de un tiempo límite preestablecido, la operatividad y la funcionalidad normal de los Sistemas de Información Misional y de Apoyo Administrativo de la Entidad.

Corresponde al Jefe de la Oficina de Sistemas, coordinar y controlar la ejecución de las actividades definidas en el Plan. Los Equipos de trabajo se estructuran conforme a los Grupos de trabajo al interior de la estructura orgánica de la Oficina



de Sistemas establecidos por la Resolución 114 de 2006; las funciones de los Equipos y las del Comité son:

### **Comité de Coordinación Administrativa y Técnica**

El Comité de Coordinación Administrativa y Técnica del PCLI está integrado por el Jefe de la Oficina de Sistemas quien lo presidirá, los Coordinadores de los Grupos de Infraestructura, de Apoyo a Sistemas de Información y de Soporte a Usuarios, dos ingenieros uno en calidad de apoyo del Jefe de la Oficina, y el otro, en calidad de Coordinador de las actividades relacionadas con la ejecución de cada una de las Fases del Plan (identificación de requerimientos, análisis de vulnerabilidades e impactos de las contingencias, desarrollo, emergencia y recuperación, prueba y administración y mantenimiento)

Administrar, mantener, coordinar y controlar la correcta implementación del **PCLI** y las actividades definidas para ejecutar antes, durante y después de la contingencia.

Dar al conocimiento del Comité Directivo del **PCL** de la **PGN**, el **PCLI** y las contingencias que se presenten en el área informática.

Mantener operativo y debidamente actualizado el Plan cada vez que entre en producción un nuevo Sistema de Información Misional o de Apoyo Administrativo o se instale una nueva versión de los mismos, que se amplíe la capacidad de los equipos, que se cambie de equipo o que se modifique las condiciones de procesamiento.

- Dar a conocer el **PCLI** a todos los funcionarios de la Oficina de Sistemas y a los usuarios de los Sistema de Información y de los Servicios Informáticos.
- Garantizar que se hayan identificado y documentado todos procedimientos y actividades necesarios para actuar durante la emergencia y restaurar la prestación de los servicios informáticos.
- Evaluar impactos de la contingencia presentada, el grado de afectación de los recursos y servicios informáticos y ordenar la activación de los procedimientos adoptados en el **PCLI** para la atención de contingencias.
- Evaluar el momento oportuno para regresar a la situación normal de operación, con base en los informes de los Equipos de Trabajo y recomendar al Comité Directivo del **PCL** de la Entidad, decisiones encaminadas a la restauración



progresiva y total de las funciones de la Oficina de Sistemas y de la consecuente prestación de los servicios informáticos.

- Diseñar y desarrollar planes de divulgación (Socialización) y entrenamiento para los funcionarios de la Oficina de Sistemas, a los usuarios de los Sistemas de Información Misional o de Apoyo Administrativo y de los Servicios Informáticos, para que conozcan y se familiaricen con los procedimientos y actividades definidos en el Plan y adquieran el entrenamiento y la habilidad requerida para su implementación.
- Registrar, conservar y actualizar la documentación del Plan.
- Apoyar logísticamente las pruebas del Plan.
- Asignar funciones a los Equipos de Trabajo.
- Establecer los controles que considere necesarios para llevar a cabo las actividades del Plan en forma confiable.

### **Funciones de los Equipos de trabajo y sus Coordinadores**

- Coordinar, supervisar y verificar que cada integrante del Equipo de Trabajo ejecute de manera eficiente, eficaz y efectiva, las actividades relacionadas con el **PCLI**, y de ser necesario, asignar tareas no definidas cuando se consideren convenientes.
- Supervisar procedimientos de respaldo y restauración.
- Coordinar la definición y ejecución de los protocolos del Plan de Pruebas del **PCLI**.
- Verificar la disponibilidad y las condiciones adecuadas de administración y seguridad de la infraestructura informática.

### **Equipo de Infraestructura**

Está conformado por el Coordinador del Grupo de Infraestructura y los funcionarios que hacen parte de este Grupo. Su Coordinador supervisa la situación en el momento de la contingencia e informa al Comité de Coordinación Administrativa y Técnica del PCLI. Este Equipo tiene las siguientes funciones:



- Definir y evaluar los procedimientos de seguridad necesarios para la conservación de los recursos informáticos y la creación, administración y almacenamiento interno y externo de las copias de respaldo de la Información Misional, el Software, la Base de Datos y la documentación correspondientes.
- Ejecutar, en el tiempo y en la forma preestablecida en el Plan, las operaciones de contingencia que le correspondan.
- Mantener actualizados el plano de la red lógica y eléctrica regulada y las especificaciones para las configuraciones de Hardware y Software de los servidores, Equipos de Red y Servicios Informáticos.
- Diseñar y mantener un plano de la configuración de la red que ha de ser implementada en el evento de una contingencia.
- Coordinar el almacenamiento externo de copias de seguridad de datos y Sistemas de Información y solicitarlas cuando se requiera.
- Definir y evaluar los procedimientos para establecer los servicios de comunicación de datos en el evento de una contingencia.
- Definir y proponer para su adopción al Comité para la Coordinación Administrativa y Técnica del PCLI, los procedimientos para el almacenamiento de material combustible en el Centro de Cómputo o en la Oficina de Sistemas, necesarios para su funcionalidad en condiciones normales de producción o de recuperación y verificar su correcta implementación.
- Mantener y optimizar los procedimientos para la recuperación ante contingencias de la funcionalidad del Centro de Cómputo.
- Participar en la instalación del Software del Sistema (al momento de la recuperación) y de la restauración de los datos junto con el Equipo de Apoyo a Sistemas de Información.
- Realizar y mantener actualizado el Inventario de Servidores, Equipos de Red, del Software Operativo y de Productividad y de los equipos electrónicos no informáticos, (UPS's, aire acondicionado y de precisión, etc.) que dan soporte al ambiente de producción de los Sistemas de Información Misional y de Apoyo Administrativo.



- Mantener la relación de los Servidores, Equipos de Red y Electrónicos no informáticos, con garantía vigente, y de los contratos vigentes de prestación de servicios de soporte y mantenimiento técnicos de esta infraestructura.
- Mantener actualizado el Directorio de Proveedores de servicios y recursos informáticos de comunicaciones, a nivel de Software y Hardware, y contactarlos en caso de contingencias.

### **Equipo de Apoyo a Sistemas de Información**

Está conformado por el Coordinador del Grupo de Apoyo a Sistemas de Información y por los funcionarios que hacen parte de este Grupo. Su Coordinador supervisa la situación en el momento de la contingencia e informa al Comité de Coordinación Administrativa y Técnica del PCLI. Este Equipo tiene las siguientes funciones:

- **Ejecutar** el programa de entrenamiento del personal involucrado (Funcionarios de la Oficina de Sistemas y de las dependencias usuarias del Sistema de Información Misional y de Apoyo Administrativo) en la ejecución del **PCLI**.
- **Definir y diseñar** estrategias de respaldo para el copiado y almacenamiento rutinario de los Sistemas de Información en producción y la Base de Datos y la documentación correspondientes.
- **Coordinar, supervisar y participar** en la ejecución de las pruebas, simulacros de emergencias y recuperación de la operatividad y funcionalidad al Sistema de Información Misional o de Apoyo Administrativo y del Software base o de productividad requeridos.
- **Planificar y establecer** los requerimientos de los Sistemas de Información Misional o de Apoyo Administrativo en cuanto a los archivos, bibliotecas, utilitarios, etc., de los sistemas operativos.
- **Mantener la relación** de los Sistemas de Información Misional o Administrativas con garantía vigente y de los contratos vigentes de prestación de servicios de soporte y mantenimiento técnicos de los mismos.
- **Mantener actualizado** el directorio de proveedores y usuarios de los Sistemas de Información Misional o de Apoyo Administrativo y contactarlos en caso de contingencias.



## Equipo de Trabajo Soporte Usuarios

Está conformado por el Coordinador del Grupo de Soporte a Usuarios y los funcionarios que hacen parte de este Grupo. Su Coordinador supervisa la situación en el momento de la contingencia e informa al Comité de Coordinación Administrativa y Técnica del **PCLI**. Este Equipo tiene las siguientes funciones:

- **Realizar y mantener** actualizado el inventario de computadores de escritorio y portátiles, impresoras y del Software operativo, de productividad y antivirus instalado en los computadores de escritorio y portátiles.
- **Establecer**, ejecutar, evaluar y actualizar los procedimientos para la atención de los requerimientos de soporte técnico que, en el evento de una contingencia, formulen los usuarios de la infraestructura informática.
- **Coordinar** con el Grupo de Atención de Emergencias de la PGN el traslado, cuando sea pertinente, de recursos informáticos.
- **Llevar** un estricto control de la documentación de las Licencias del recurso informático adquirido por la PGN.
- **Mantener** la relación de los computadores de escritorio, de los portátiles y de las impresoras con garantía vigente y de los contratos vigentes de prestación de servicios de soporte y mantenimiento de esta infraestructura.
- **Realizar y mantener** actualizado el directorio de los contactos de los proveedores de los computadores de escritorio y portátiles, las impresoras, del software operativo, de productividad y antivirus y contactarlos en caso de contingencia.
- **Definir**, solicitar, administrar y disponer en lugar adecuado, un stock mínimo de partes de los computadores de la Entidad.

### 6.3.2. Análisis de Riesgos - Análisis de vulnerabilidades e impactos de las contingencias

El análisis de riesgos, se realizó con base en las contingencias inherentes o propias de la disponibilidad, uso y operación de la infraestructura informática que, en general, son provocadas por las siguientes situaciones:



### **Eventos naturales**

- Inundaciones
- Vientos
- Movimientos Sísmicos
- Descargas eléctricas

### **Actos provocados por terceros (Empleados o externos)**

- Terrorismo
- Asaltos o toma de las instalaciones
- Disturbios civiles
- Robo
- Fraude
- Sabotaje (Interrupción de los servicios, virus informáticos, etc.)

### **Actos accidentales o por omisión**

- Incendio
- Explosiones
- Falla en los Servidores
- Falla en los equipos activos de Red
- Falla en el fluido eléctrico
- Falla en los canales de comunicaciones
- Falla en el Software aplicativo (Aplicaciones Misionales y de Apoyo)
- Falla en el Software Base (Operativo, de productividad, de comunicaciones, etc.)
- Borrado de información y/o de la Base de Datos

Tarea 1. Identificar los Escenarios o Fuentes de Riesgo en relación con los recursos y servicios informáticos.

Tarea 2. Identificar los Riesgos asociados con cada uno de los escenarios o factores críticos, teniendo en consideración los siguientes criterios: importancia institucional del recurso o servicio informáticos, la probabilidad de ocurrencia de los riesgos asociados y su probable impacto en la continuidad de las operaciones, la prioridad de la atención de la contingencia, las estrategias y procedimientos de control y el equipo responsable de las mismas; los escenarios son:

- Base de datos
- Centro de Cómputo
- Equipos servidores de comunicaciones y canales
- Computadores de la Entidad
- Equipos electrónicos no informáticos
- Software aplicativo, operacional y de ofimática



- Servicios de Comunicación
- Suministros de formas continuas y especiales, medios magnéticos, etc.
- Archivos maestros y de movimientos considerados críticos

### 6.3.3. Desarrollo

Además de la especificación de los procedimientos para desarrollar cada una de las estrategias contingentes, en esta Fase se generó la documentación del Plan y se definieron los procedimientos a adoptar para la vuelta a la normalidad, es decir, la reconstrucción de la situación inicial antes de la contingencia.

Tarea 1 Especificar procedimientos para el desarrollo de cada una de las estrategias contingentes seleccionadas.

Tarea 2 Definir políticas de Backups (copia de respaldo) para los Servidores y los procedimientos para su registro y control.

Las siguientes son algunas de las políticas definidas para Backups de los Servidores:

- Uso obligatorio de un Formulario Estándar para el registro y control de los Backups, sus periodicidades, tipo y clase.
- Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups incrementales).
- Reemplazo de los Backups, en forma periódica.
- Almacenamiento de los Backups en condiciones ambientales óptimas y en sitios diferentes al Centro de Cómputo (Para evitar la pérdida total si la contingencia afecta estas instalaciones).
- Pruebas periódicas de los Backups, verificando su funcionalidad mediante la comparación contra resultados anteriores confiables.

### 6.4. Emergencia y Recuperación

En esta fase se desarrollaron los procedimientos que los Equipos de Trabajo del **PCLI** realizarán en caso de emergencia:

Tarea 1. Evaluación de daños.



Describir, evaluar y calificar los daños que la contingencia ocasionó en las instalaciones del Centro de Cómputo y/o recursos o servicios informáticos y determinar la capacidad operacional remanente, con base en los siguientes criterios:

- **Masiva:** El daño a las instalaciones y a los recursos y servicios informáticos se puede considerar total, dado que la capacidad operacional remanente es menor del 30%; ello equivale a una operatividad y funcionalidad del Centro de Cómputo y/o recursos o servicios informáticos prácticamente nulos.
- **Menor e Importante:** El daño a las instalaciones y a los recursos y servicios informáticos se puede considerar en este nivel cuando la capacidad operacional remanente es mayor de 30% y menor de 90%; ello equivale a unas operatividad y funcionalidad del Centro de Cómputo y/o recursos o servicios informáticos recuperables en un tiempo mínimo de dos (2) días.
- **Menor y leve:** El daño a las instalaciones y a los recursos y servicios informáticos se puede considerar en este nivel cuando la capacidad operacional remanente está entre el 90% y el 100%; ello equivale a una operatividad y funcionalidad del Centro de Cómputo y/o recursos o servicios informáticos fácil y rápidamente recuperables.
- **Identificar** qué recursos y servicios informáticos han sido afectados, qué equipos han quedado no operativos y cuáles de ellos se pueden recuperar.

## Tarea 2. Ejecución de Actividades del **PCLI**

En el marco de la ejecución de las actividades definidas en el **PCLI** se adelantarán los trabajos de recuperación en dos (2) etapas:

**La primera**, para restaurar la funcionalidad y operación de los Sistemas de Información Misional y de Apoyo Administrativo y la prestación de los servicios informáticos.

**La segunda**, para que el Centro de Cómputo cuente con los recursos informáticos necesarios y recupere su operatividad normal que garanticen el procesamiento y funcionalidad de los Sistemas de Información Misional y de Apoyo Administrativo y la prestación de los servicios informáticos de manera eficiente y efectiva.

A partir del momento en que se haga manifiesta una situación de emergencia (Incendio, explosión u otro evento mayor) en el Centro de Computo, y determinado un porcentaje de afectación de las instalaciones físicas y técnicas con las que se cuenta, menor del 50%, se realizarán inmediatamente los procedimientos para la recuperación, los que continuarán hasta que se restauren



los servicios de procesamiento de datos en el mismo Centro de Cómputo, debido a que la Procuraduría, actualmente, **no dispone de un Centro Alterno** para el procesamiento de datos.

Los procedimientos son responsabilidad de cada Equipo de Trabajo, teniendo en cuenta que la prioridad más alta es la seguridad de los empleados, lo que significa que si la naturaleza del desastre no da tiempo para apagar y evacuar, el personal debe salir inmediatamente del Centro de Cómputo o área afectada, caso en el cual se debe notificar inmediatamente al Comité de Emergencias - CREA. En caso contrario, se deben realizar las siguientes actividades:

- En caso de **Orden Formal** de evacuación de las instalaciones de la Procuraduría General de la Nación, hacerlo en forma ordenada y ágil, por Las Rutas destinadas para ello en el Plan de Evacuación del Personal y atendiendo las instrucciones de los Brigadistas y/o de los Coordinadores de Evacuación de la Oficina de Sistemas, conforme a los procedimientos establecidos en el Plan de Emergencias adoptado por la Entidad.
- Dar inicio a los procedimientos establecidos en el Plan de Emergencias, por ejemplo, usar los elementos disponibles para atender la contingencia, tales como extintores, etc.
- Contactar a bomberos y policía, de ser necesario y a los entes de apoyo externo que se requieran.
- De ser posible, enviar un correo electrónico con el mensaje "**Apague y desconecte de inmediato los computadores e impresoras**".
- Ejecutar procedimientos de apagado y desconexión de los Servidores, Periféricos y demás dispositivos eléctricos o electrónicos.
- Poner en **OFF** el Circuito Principal de corriente eléctrica de la Oficina de Sistemas.
- Apagar luces y bajar tacos en las cajas de distribución
- Iniciar, cada coordinador de Equipo de Trabajo del **PCLI**, un árbol telefónico para contactar a todos los miembros de su Equipo.
- El Comité de Coordinación Administrativa y Técnica hará una apreciación inicial de la extensión de la emergencia tan rápido como sea posible y



decidirá iniciar o no los procedimientos de recuperación en las mismas instalaciones del Centro de Cómputo.

- Contactar al Comité Directivo del **PCL** de la Procuraduría General de la Nación, a los proveedores de los recursos y servicios informáticos afectados y a los usuarios de estos recursos y servicios.
- El Comité de Coordinación Técnica y Administrativa convocará a los coordinadores de los Equipos de Trabajo e iniciará la coordinación de la ejecución de los procedimientos para la recuperación del Centro de Cómputo y los servicios informáticos, dentro de los siguientes parámetros:

Dentro de las 24 horas siguientes a la emergencia se debe:

- Informar a los usuarios acerca de las condiciones operativas y funcionales de los Sistemas de Información y los Servicios Informáticos y dar un tiempo estimado para la recuperación.
- Contactar a los proveedores de recursos informáticos y servicios de soporte técnico tanto de Hardware como de Software.
- Ejecutar las actividades definidas para la recuperación de los servicios, en coordinación con los proveedores de los recursos o servicios informáticos en garantía o con contrato de soporte y mantenimiento técnico, y con los usuarios de los Sistemas de Información.

Dentro de los 2 días siguientes a la emergencia se debe:

- Establecer las prioridades de recuperación de servicios críticos para la Entidad.
- Disponer los requerimientos de personal, técnicos y logísticos necesarios.
- Concluir la realización de los procedimientos para la recuperación.
- Iniciar la implantación por fases de la Red de Comunicación de datos.

Dentro de los 4 días siguientes a la emergencia se debe:

- Restaurar las copias de respaldo (Backups) de datos.
- Evaluar los Sistemas en Línea, para verificar la operación y validez de los datos restaurados.



- Notificar a los usuarios el estado de la recuperación.

Dentro de los 28 días siguientes a la emergencia se debe:

- Asegurar la operación total de los sistemas críticos.
- Restaurar completamente la Red de Comunicación de Datos y las operaciones.

#### Tarea 3. Evaluación de Resultados.

Una vez concluidas las labores de recuperación y prestación de los servicios informáticos afectados, el Comité de Coordinación Administrativa y Técnica desarrollará las siguientes actividades:

Evaluar los resultados de la recuperación y de todas las actividades realizadas.

Recomendar al Comité Directivo del **PCL** de la Procuraduría General de la Nación, volver a la situación normal en el Centro de Cómputo, previo cumplimiento de las siguientes condiciones:

- El peligro que ocasionó la contingencia desapareció completamente.
- Las instalaciones físicas del Centro de Cómputo están debidamente acondicionadas.
- Los Servidores y Equipos activos de la Red, ubicados en el Centro de Cómputo, fueron debidamente instalados y probados y se verificó su correcto funcionamiento.
- Los Sistemas de Información y Base de Datos fueron instalados, restaurados y probados satisfactoriamente.
- Las instalaciones eléctricas y el aire acondicionado que requiere el Centro de Cómputo se encuentran en condiciones adecuadas de funcionamiento.
- Se comunicó oportunamente a los usuarios el inicio de los procesos normales.

#### Tarea 4. Reporte al Comité de Administración.

De la evaluación de la contingencia y de los resultados de la aplicación del **PCLI**, los Equipos de Trabajo presentarán informe escrito al Comité de Coordinación



Administrativa y Técnica, en el que incluirán recomendaciones para optimizar el **PCLI**.

## 6.5. Prueba

El Plan de Pruebas definido por la Oficina de Sistemas con el propósito de probar y certificar la operatividad del **PCLI**, contempla los siguientes objetivos generales y específicos:

### 6.5.1 General

Determinar la operatividad del **Plan de Contingencias Logísticas Informáticas**, es decir, qué tan funcional, correcto y pertinente es para recuperar el procesamiento de datos y minimizar el impacto negativo de la contingencia presentada y qué partes del mismo es necesario mejorar.

### 6.5.2 Específicos:

- **Identificar y corregir** fallas en el Plan de Contingencias Logísticas Informáticas.
- **Validar** la consistencia de los procedimientos definidos para casos de recuperación de contingencias.
- **Facilitar** la divulgación y el entrenamiento en los procedimientos y protocolos de recuperación.
- **Motivar** a los funcionarios involucrados en el diseño y desarrollo del Plan a mantener actualizados los procedimientos pertinentes.
- **Verificar** que la documentación del Plan de Contingencias Logísticas Informáticas sea completa y pertinente.
- **Evaluar** la consistencia, integridad y grado de usabilidad de la información almacenada en las copias de seguridad para la recuperación de la operatividad de los Sistemas de Información misionales y administrativos, en caso de emergencia.
- **Determinar** la oportunidad y capacidad de reacción de la Oficina de Sistemas ante la contingencia presentada.
- **Evaluar la habilidad**, entrenamiento y rendimiento del personal involucrado en la ejecución del Plan de Contingencias Logísticas Informáticas.



- **Evaluar la coordinación** entre los Equipos de Trabajo definidos dentro del Plan de Contingencias Logísticas Informáticas.

Tarea 1. Definir las pruebas a probar por cada una de las contingencias.

Tarea 2. Definir los procedimientos a desarrollar por cada una de las pruebas.

Tarea 3. Generar la información documentada producto de la aplicación del Plan de Pruebas.

Como resultado de la definición y aplicación del Plan de Pruebas, se obtendrá la siguiente información:

- Protocolos o Esquemas actualizados de las prueba.
- Resultados obtenidos de la aplicación de los Protocolos o Esquemas de prueba al **PCLI**.
- Evaluación y Conclusión acerca de la funcionalidad, corrección y pertinencia del **PCLI**.
- Determinación del período crítico de recuperación, es decir, el tiempo máximo en el que la Oficina de Sistemas debe reanudar el procesamiento de datos.
- Cronograma para el ajuste del **PCL**.

## **6.6. Administración y Mantenimiento**

Una vez adoptado institucionalmente el Plan de Contingencias Logísticas Informáticas, la Oficina de Sistemas realizará revisiones y actualizaciones al mismo, cada tres (3) meses, con los propósitos de observar su grado de adecuación y actualidad respecto de los cambios y verificar su efectividad para asegurar que las capacidades de procesamiento de información puedan ser reanudadas rápidamente luego de una interrupción imprevista.

Tarea: Definir procedimientos para:

- Ejecutarlo
- Revisarlo
- Actualizarlo
- Probarlo
- Socializarlo, sensibilizar y entrenar a los funcionarios en su implementación.



**Responsables:**

Secretario General  
Jefe de Oficina de Sistemas  
Coordinador Grupo de Infraestructura  
Coordinador Grupo de Soporte a Usuarios  
Coordinador Grupo de Apoyo Sistemas de Información  
Coordinador Grupo de Archivo  
Administrador de Servidores  
Administradores Técnicos Sistemas de Información  
Interventores  
Supervisor Contrato de Conectividad