CONTRATO INTERADMINISTRATIVO No. 256 DE 2017

DOCUMENTO PLAN DE CONTINGENCIA PARA SISTEMA SIGEP

PROYECTO: RENOVACIÓN DE PORTALES WEB Y MICROSITIOS DE FUNCIÓN PÚBLICA E IMPLEMENTACIÓN DE LA SEGUNDA FASE DE LA ESTRATEGIA DE GOBIERNO EN LÍNEA PARA LA ENTIDAD

V 1.0

Diciembre de 2017

CINTEL
Carrera 14 No. 99-33/55 Oficina 505 Edifício Torre REM, Tel: 6404410
Fax: 6401094/58
Bogotá D.C.

TABLA DE CONTENIDO

ÍNDICE DE GRAFICAS

ÍNDICE DE TABLAS

DOCUMENTO PLAN DE CONTINGENCIA

HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción del Cambio	Responsable
12/2017	1_0	Primera versión del Documento de plan de contingencia	CINTEL

1. INTRODUCCIÓN

Función Pública está desarrollando la Estrategia de Gobierno en Línea (Gobierno Digital) plasmada en el Decreto Único Reglamentario del sector de Tecnologías de la Información y las comunicaciones 1078 de 2015, donde se han tenido en cuenta la necesidad de contemplar planes de contingencia para sus sistemas misionales de acuerdo con las directrices emanadas del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) en su circular No.002 del 06 de julio de 2011.

En el entorno de las tecnologías de la información se encuentran amenazas significativas que pueden ser incidentes menores o catastróficos que afecten la labor normal de Función Pública, en dado caso que se presenten alguno de estos aspectos, se genera la necesidad de una recuperación en el menor tiempo posible de las labores, garantizando la continuidad de los servicios que ofrece Función Pública tanto interno como externo.

El plan de continuidad se crea e implementa para responder ante situaciones que interrumpen el normal funcionamiento de los servicios de Función Pública, es una herramienta que ayuda a mitigar el riesgo de no disponibilidad de los recursos tecnológicos para la normal realización de las labores.

El presente documento corresponde plan de contingencia para el sistema de información de gestión del empleo público - SIGEP, permitiendo identificar las acciones necesarias para reestablecer la operación de los sistemas.

2. OBJETIVO GENERAL

Establecer el plan de contingencia para el Sistema SIGEP en caso de una falla que genere una indisponibilidad del sistema por un tiempo mayor al establecido en los Acuerdo de Nivel de Servicio(ANS).

2.1 OBJETIVOS ESPECÍFICOS

Para este plan se han establecido los siguientes objetivos:

1. Definir roles y responsables para las acciones de contingencia.
2. identificar riesgos y vulnerabilidades para el sistema de información.
3. Establecer las actividades para cada etapa del plan de contingencia.

3. ALCANCE

Este Plan de Contingencia está desarrollado para simular la caída de elemento tecnológico hardware o software cuyo tiempo de restauración supera el ANS siendo por tanto necesario activar los elementos de contingencia. La contingencia se activa al presentarse una falla que haga imposible la recuperación del Sistema de información SIGEP en ambiente de producción.

Para el presente plan se parte del supuesto de una falla en las bases de datos y en el servidor de aplicaciones del sistema de información SIGEP en el ambiente de producción.

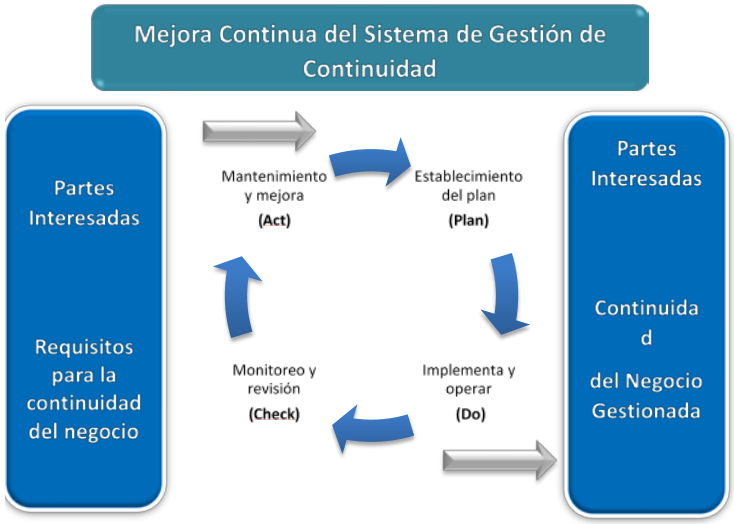
Se establece que para el plan de contingencia no se completa una contingencia para la información de anexos que hacen parte del sistema de información SIGEP. Por lo cual se debe contemplar la inactivación de las funcionalidades que afectan estos objetos. No funcionará la consulta ni la edición.

Por otro lado, el servicio de tareas programadas estará excluido del presente plan de contingencia. Esto afecta el proceso de cierre de contratos y la interoperabilidad con el servicio de distrito (SIDEAP).

4. METODOLOGÍA

El estándar utilizado para la implementación de la continuidad de negocios en la OTI es la norma ISO 22301:2012, esta norma determina actividades específicas para el desarrollo de la continuidad del servicio, la norma propone desarrollar dichas actividades mediante un ciclo de mejora continua similar al Ciclo de Deming o modelo PDCA, por sus iniciales en inglés, que traducido al español se denomina modelo PHVA (Planear, Hacer, Verificar y Actuar), y se recomienda aplicarlo para gestionar la continuidad del negocio según lo establecido en la siguiente gráfica.

Gráfica 1- Ciclo PHVA



Fuente: Norma ISO 22301:2012 página VI

A continuación las definiciones de cada una de las etapas y sus complementos, y los objetivos que llevan a la continuidad según lo explica la norma ISO 22301:2012 en su introducción (página vi).

Planear: Se establecen los objetivos y las actividades necesarias para generar un sistema de gestión de continuidad y proporcionar resultados de acuerdo con las necesidades de la organización y sus usuarios, alineados a los objetivos estratégicos del negocio.

Hacer: Se implementa y se transforma en operativo el sistema de continuidad teniendo en cuenta la política, los procesos, los controles y demás procedimientos.

Verificar: Se monitorea y mide el sistema de continuidad teniendo en cuenta la política, los procesos, los controles y demás procedimientos reportando los resultados a la dirección para su revisión y determinar acciones correctivas y de mejora.

Actuar: Se emprenden las acciones necesarias para mejorar continuamente el Sistema de Gestión de la Continuidad teniendo en cuenta los resultados de

la revisión realizada por la dirección y los cambios que puedan aparecer del alcance, la política y los objetivos de continuidad.

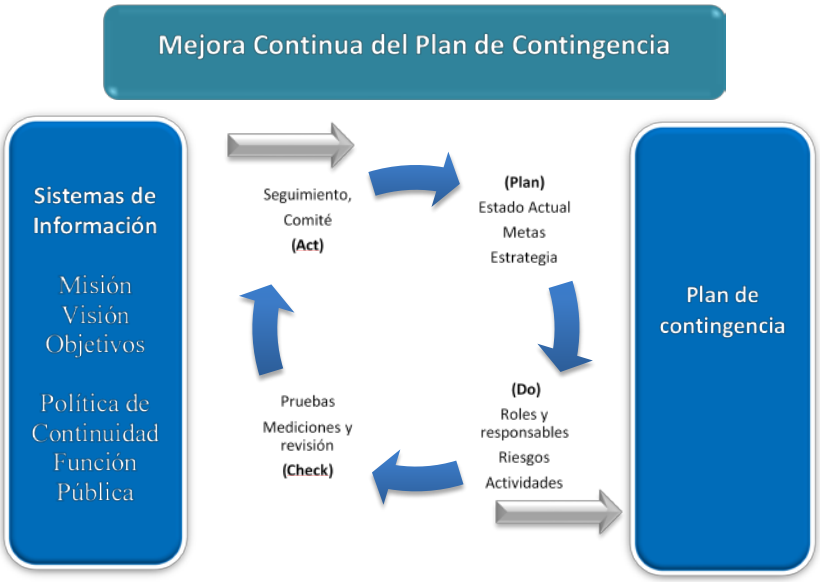
Entradas: Los usuarios, personas involucradas en los procesos del negocio y los requisitos para la continuidad del negocio se basan en los temas internos y externos que son relevantes para el propósito de la organización y que se definen en su visión, misión, objetivos y que son tenidos en cuenta en la Política de Continuidad.

Salidas: La continuidad del negocio de los procesos críticos.

Mejora Continua: La mejora continua son todas las acciones, realizadas a lo largo del ciclo de vida, para aumentar la eficacia, la eficiencia y brindar beneficios tanto a la organización como a sus partes interesadas. Una organización puede mejorar a través de la aplicación de la política de continuidad de negocio, los objetivos, los resultados de auditorías, el análisis de eventos controlados, los indicadores, las acciones correctivas y preventivas y la revisión por la dirección.

A partir de lo anterior, la siguiente grafica ilustra la aplicación del ciclo PHVA al presente plan de contingencia, permitiendo definir acciones en cada una de las fases del ciclo y permitiendo también la mejora continua del plan.

Gráfica 2. Aplicación de ciclo PHVA al plan de contingencia



Fuente: CINTEL-2017

El desarrollo de la metodología tiene como punto de partida el Plan de Continuidad de Función Pública, bajo los principios y lineamientos definidos en este plan se estructura el plan de contingencia para el Sistema Misional SIGEP

5. FASE 1: PLANEAR

En fase tiene como objetivo planear la estrategia para el plan de contingencia, donde se inicia con la introducción del contexto que enmarca el sistema de información, el punto de partida es el plan de continuidad de la Entidad, luego se define el objetivo del plan de contingencia para el Sistema de Información SIGEP y finalmente se realiza una descripción del estado actual del sistema de información. Una vez se establece el contexto del sistema de información se realizarán las siguientes actividades:

- Definir roles y responsabilidades.
- Establecer las políticas de respaldo de la información.
- Identificar riesgos y vulnerabilidades del sistema de información.
- Definir las actividades de contingencia para el sistema de información.

5.1 PLAN DE CONTINUIDAD DE FUNCIÓN PÚBLICA

Función Pública con el objetivo de definir las actividades preventivas, defectivas y correctivas para reaccionar de manera eficiente ante una eventualidad que comprometa el desarrollo de las actividades cotidianas, la seguridad del personal o la prestación del servicio cuenta con un plan de continuidad.

El plan de continuidad de la Entidad se encuentra descrito en el documento: Documento Técnico del Plan de Continuidad del Negocio[1], de donde se abstrae el siguiente apartado: "Con el fin de contar con una herramienta que permita prevenir o reaccionar adecuadamente ante posibles incidentes que pongan en riesgo a los *Servidores Públicos*, afectar el debido *desarrollo de las actividades* propias de Función Pública, impedir *la prestación y continuidad del servicio* a los Grupos de Valor o el *cumplimiento de los compromisos* establecidos en la planeación estratégica, la Entidad consolidó una serie de acciones a emprender en el *Plan de continuidad del negocio* que, diseñadas y ejecutadas de forma planificada, permitirían responder de manera eficiente ante una

[1] Función Pública (Marzo 2017), Documento Técnico del Plan de Continuidad del Negocio, extraído de http://www.funcionpublica.gov.co/documents/418537/528603/Documento+T%C3%A9cnico+plan+de+continuidad+del+Negocio/dda1f666-0ca1-4375-b60e-e69547fe26e5. Diciembre 2017

eventualidad, restablecer en menor tiempo la prestación de los servicios y mitigar el impacto negativo de la pérdida de recursos."

A partir de este principio se genera el siguiente plan de contingencia, el cual contempla los lineamientos y objetivos específicos del plan de continuidad de Función Pública

5.2 PLAN DE CONTINGENCIA PARA EL SISTEMA DE INFORMACIÓN SIGEP

El presente plan de contingencia a partir de una falla de la base de datos y del servidor de aplicaciones del ambiente de producción del sistema de información SIGEP establece las actividades a desarrollar hasta llegar a reestablecer el servicio.

Este Plan de Contingencia reúne un conjunto de actividades que facilitarán mantener el normal funcionamiento del sistema de información SIGEP de Función Pública, cuando este se vea afectado negativamente por causa de algún incidente de índole interno o externo.

Dado que los sistemas que hacen parte del alcance del plan de contingencia son de carácter misional para la Entidad se tienen en cuenta los siguientes lineamientos:

- Mantener la información asequible.
- Minimizar el impacto y perdidas ante un desastre.
- Documentar el proceso de recuperación ante un desastre.
- Mantener en funcionamiento los procesos misionales de la Entidad.
- Mantener la continuidad de la información.

Para la realización del presente plan de contingencia se contempla:

- **Estado actual**: se tiene como punto de partida la descripción del estado actual del sistema de información, donde se identifican los componentes tecnológicos del sistema.
- **Meta**: La meta del plan de contingencia es establecer los roles y responsables del sistema para la acción de contingencia, definir las actividades a realizar con la respectiva estimación de tiempos para el desarrollo.

- **Estrategia**: Este plan de contingencia se establece desde la eventualidad de una falla del sistema de información en su ambiente de producción para lo que se define como estrategia para la recuperación del servicio utilizar como escenario de contingencia realizar las acciones necesarias para utilizar el ambiente de capacitación durante el tiempo que requiere para reestablecer el servicio en el ambiente de producción.

5.3 DESCRIPCIÓN DEL ESTADO ACTUAL DEL SISTEMA DE INFORMACIÓN SIGEP

El Sistema de Información SIGEP es un Sistema de Información y Gestión del Empleo Público al servicio de la administración pública y de los ciudadanos. Contiene información de carácter institucional tanto nacional como territorial, relacionada con: tipo de entidad, sector al que pertenece, conformación, planta de personal, empleos que posee, manual de funciones, salarios, prestaciones, etc.; información con la cual se identifican las instituciones del Estado colombiano.[2]

Igualmente, el sistema contiene información sobre el talento humano al servicio de las organizaciones públicas, en cuanto a datos de las hojas de vida, declaración de bienes y rentas y sobre los procesos propios de las áreas encargadas de administrar al personal vinculado a éstas.

Gráfica 3. Imagen portal Sistema misional SIGEP

Fuente: Portal SIGEP- 2017.

[2] Qué es sigep http://www.sigep.gov.co/que_es

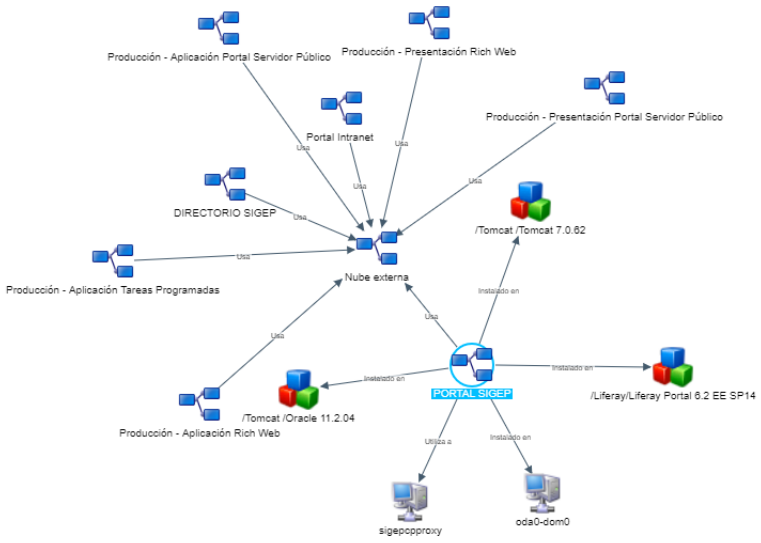
El SIGEP es a su vez, una herramienta de gestión para las instituciones públicas, al permitirles adelantar con base en la información del sistema y la viabilidad de este, procesos como la movilidad de personal, el Plan Institucional de Capacitación, evaluación del desempeño, programas de bienestar social e incentivos.

El Sistema de Información SIGEP está compuesto por un portal(sigep.gov.co), donde la gestión de contenidos se realiza por LIFERAY el cual contiene los portales de servidores y contratistas, y la visualización de consultas y reportes. Adicionalmente contiene un enlace de acceso al sistema de información SIGEP(gestión.sigep.gov.co), que es el portal de las entidades también denominado RichWeb.

5.4 IDENTIFICACIÓN DE LA INFRAESTRUCTURA

El Plan de Contingencia para SIGEP de Función Pública abarca todos los elementos que hacen parte de los servicios tecnológicos que hacen parte del servicio. A partir de la información suministrada a través de la herramienta de mesa de servicio se ilustra la infraestructura en la siguiente gráfica.

Gráfica 4. Modelo de Infraestructura Sistema información SIGEP



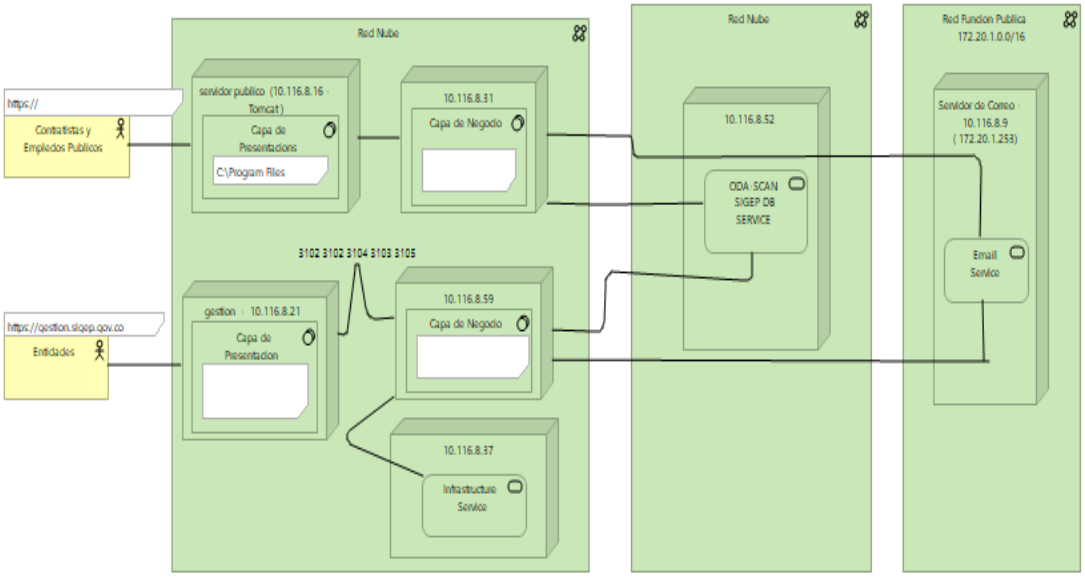
Fuente: http://servicedesk.dafp.gov.co/herramienta de mesa de servicio- 2017.

SIGEP está compuesto por los siguientes ambientes:

- Producción
- Preproducción
- Pruebas
- Capacitación

La arquitectura del sistema de información n SIGEP en su ambiente de producción se ilustra en la siguiente gráfica.

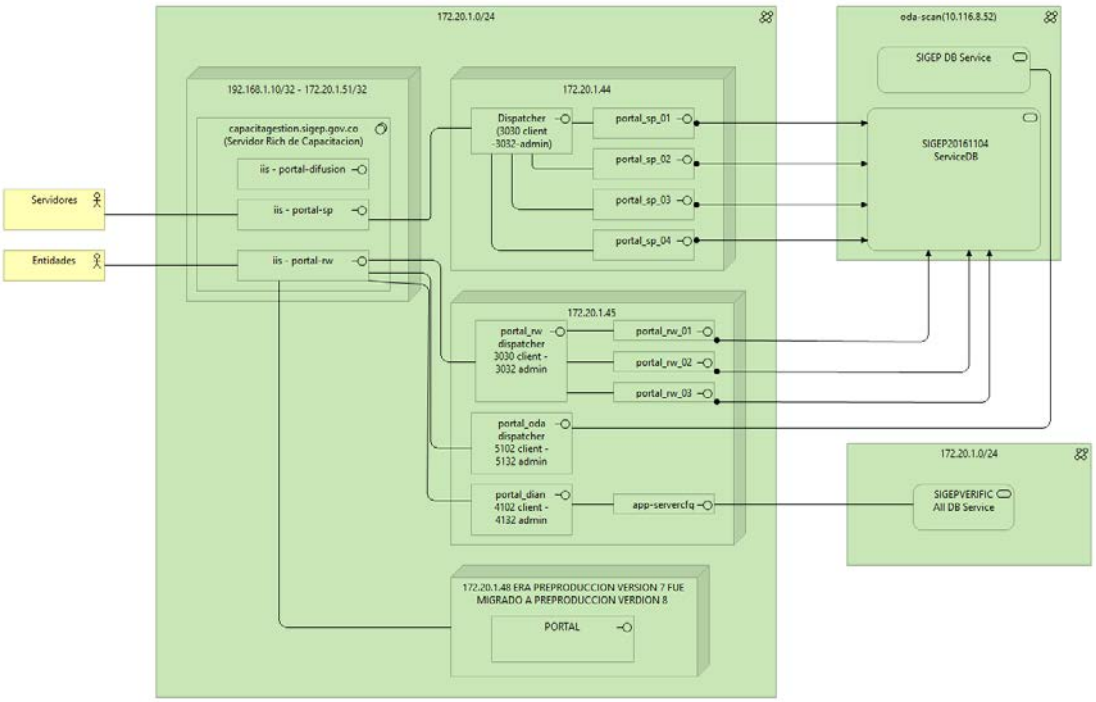
Gráfica 5. Ambiente de producción - Nube



Fuente: Función Pública-2017

El ambiente de producción se encuentra alojando en la nube privada. Para el ambiente de capacitación se tiene la siguiente arquitectura y se encuentra alojado en el centro de cómputo de la Entidad

Gráfica 6. Ambiente de capacitación– Centro de Cómputo Función Pública



Fuente: Función Pública-2017

5.5 SERVIDORES

El servidor asociado al portal SIGEP de Función Pública es: DAFPAP05.

El servidor tiene las siguientes características:

Tabla 1. Características de máquina virtual

SERVIDOR	TIPO	DESCRIPCIÓN
DAFPAP05 10.116.8.19	Hardware	Disco Duro 800G Memoria RAM 32G Procesamiento: 8vCPU * 64bits
	Sistema operativo	Red Hat Enterprise Linux Server release 7.2 (Maipo)
	Aplicación	tomcat7 liferay

Fuente: CINTEL-2017

Esta información descriptiva como componente del sistema de información SIGEP.

Los servidores asociados al sistema de información SIGEP de Función Pública son:

- Servicio Web Meta4 (richweb): DAFPPR01.
- Servicio Web Meta4 (richweb): DAFPPR02.
- Servicio Web Meta4 (portalsp): DAFPAP01.
- Servicio Web Meta4 (portalsp): DAFPAP03.
- Servicio Tareas programadas: DAFPAP04.
- Servicio de archivos: DAFPAP08.

Los servidores tienen las siguientes características:

Tabla 2. Características de máquina virtual

SERVIDOR	TIPO	DESCRIPCIÓN
DAFPAP01 10.116.8.21	Hardware	Disco Duro 800G Memoria RAM 32G Procesamiento: 8vCPU * 64bits
	Sistema operativo	Windows Server 2012
DAFPPR01 10.116.8.16	Hardware	Disco Duro 800G Memoria RAM 32G Procesamiento: 8vCPU * 64bits
	Sistema operativo	Windows Server 2012
DAFPAP02 10.116.8.59	Hardware	Disco Duro 800G Memoria RAM 32G Procesamiento: 8vCPU * 64bits
	Sistema operativo	Windows Server 2012
DAFPAP03 10.116.8.31	Hardware	Disco Duro 800G Memoria RAM 32G Procesamiento: 8vCPU * 64bits
	Sistema operativo	Windows Server 2012
DAFPAP04 Tareas Programadas 10.116.8.32	Hardware	Disco Duro 800G Memoria RAM 32G Procesamiento: 8vCPU * 64bits
	Sistema operativo	Windows Server 2012
DAFPAP08 Servidor de archivos 10.116.8.37	Hardware	Disco Duro 120Gbytes - 5Tbytes Memoria RAM 4G Procesamiento: 4vCPU * 64bits
	Sistema operativo	Windows Server 2012

Fuente: CINTEL-2017

5.6 BASES DE DATOS

La instancia de base de datos asociada al Sistema de información SIGEP de Función Pública es jdbc:oracle:thin:@//oda-scan:1521/SIGEP.

5.7 SOFTWARE BASE DEL DISEÑO DE ARQUITECTURA DEL SISTEMA DE INFORMACIÓN

El software base para el sistema de información SIGEP se enlista en las siguientes tablas:

Tabla 3. Software base Portal SIGEP

CAPA	SOFTWARE BASE PORTAL
Presentación	Tomcat 7. 0.62 Liferay Portal 6.2 EE SP14
Bases de datos	Oracle 11.2.04

Fuente: CINTEL-2017

Tabla 4. Software base sistema SIGEP

CAPA	SOFTWARE BASE SISTEMA
Presentación	Tomcat 8.0.28
Aplicación	Peoplenet8(tecnología propietaria) lenguaje de programación LN4
Bases de datos	Oracle 11.2.04

Fuente: CINTEL-2017

5.8 ESTRATEGIA DE CONTINGENCIA

A partir de la identificación de la infraestructura asociada al sistema de información SIGEP se establece como escenario de contingencia el ambiente de capacitación, de lo anterior se genera la relación que se muestra en la siguiente tabla para la ejecución del presente plan.

Tabla 5. Relación ambiente de producción y escenario de contingencia

	AMBIENTE DE PRODUCCIÓN	ESCENARIO DE CONTINGENCIA AMBIENTE DE CAPACITACIÓN
Aplicación Portal servidores	10.116.8.31 DAFPAP03	172.20.1.44 SIGEPCA01-CAP

	AMBIENTE DE PRODUCCIÓN	ESCENARIO DE CONTINGENCIA AMBIENTE DE CAPACITACIÓN
Presentación	10.116.8.16 DAFPPR01 10.116.8.21 DAFPAP01	172.20.1.51 SIGEPCA-CAP
Aplicación Rich	10.116.8.59 DAFPAP02	172.20.1.45 SIGEPCA02-CAP
Bases de datos	Oda-scan:1521/SIGEP	SIGEPVERIFIC/DB

Fuente: CINTEL- 2017

- **Copias de seguridad.** Para el escenario de contingencia se contempla una restauración de la información de las bases de datos en el ambiente de producción, lo anterior permitirá operar en el ambiente de contingencia con información a su última actualización. Las copias de respaldo de las bases de datos se encuentran alojadas en el servidor cronos.

Tabla 6. Ubicación de copias de respaldo para bases de datos en producción

TIPO	NODOS	DESCRIPCION	EXPORT (periodicidad)	DEPURACIÓN
DB PRODUCCION	CRONOS-2	BD de producción **SQLServer**	Fullexport incremental (diario) y Full backup (Semanal)	Full backup con log (semanal)
ARCHIVOS (DATA) DE BASES DE DATOS				
TIPO	**NODOS**	**DESCRIPCION**	**SISTEMA OPERATIVO**	**RUTA FILE SYSTEM (periodicidad)**
EXPORT DB_ODA	YAKSA-2	EXPORT BD **ORACLE**	WIN2012 R2	YAKSA-2\G:\DBA\oda_scan (FULL-SEMANAL)

Fuente: Función Pública, Políticas de Respaldo, Custodia y Recuperación de la Información-2017

- **Versión de software instalado**. Para el presente plan de contingencia se contempla que tanto el ambiente de producción como el escenario de contingencia, en este caso, el ambiente de capacitación cuenta con las mismas de versiones de software para garantizar la compatibilidad de copias de seguridad.

6. FASE 2: HACER

En esta fase se definirán los roles y responsabilidades para el sistema de información, se va a identificar las vulnerabilidades asociadas y se definirán las actividades necesarias para el restablecimiento del servicio.

6.1 ROLES Y RESPONSABILIDADES

Para asegurar la acertada implementación y gestión de la continuidad de los servicios tecnológicos se deben establecer roles y responsabilidades que involucren las áreas de gestión en el departamento de Tecnologías de la información.

Tabla 7. Responsables plan de contingencia sistema de información SIGEP

Rol	Ubicación	Teléfono-ext	Responsable	Celular
Administradores de Servidores	Departamento Administrativo de la Función Pública – Piso 5	508 504	Edwin Vargas Ana Castro	3103189100 3013059469
Administradores de redes y Comunicaciones	Departamento Administrativo de la Función Pública – Piso 5	507	Leonardo Calderón	3102840195
Administrador SIGEP	Departamento Administrativo de la Función Pública – Piso 5	505 200 517	Lina Escobar Francisco Urbina Rafael Rodríguez	3174031509 3125480756 3178548956
Proveedor* Soporte Básico META4	META4	6739744	Gerente Soporte y Base Instalada	
Proveedor* Soporte Extendido-HEINSONH	Departamento Administrativo de la Función Pública – Piso 5 Gerente proyecto HEINSOHN	505 6337070 / 9512	Desarrollador en Sitio Olga Tapias	 3002205247
Administrador DBA	Departamento Administrativo de la Función Pública – Piso 5	517	Rafael Rodríguez	3178548956

*Se debe validar el contrato vigente con los proveedores

Fuente: CINTEL-2017

6.2 POLÍTICAS DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN

Función Pública cuenta con una política de respaldo, almacenamiento y recuperación de la información crítica que garantiza la disponibilidad e integridad de los activos informáticos dispuestos en el centro de datos de su sede principal.

Esta política aplica a todos los sistemas de información y dispositivos de almacenamiento de datos que contengan información catalogada como critica para la prestación de servicios internos y externos del Departamento Administrativo de la Función Pública alojada en los servidores del centro de datos Ubicado en la sede principal del Departamento Administrativo de la Función Pública.[3]

Función Pública realiza copias de seguridad de la información de en disco y en cintas, las cuales se entregan en custodia a un tercero. Las bases de datos tienen rutinas de realización de copias de seguridad diaria, para las máquinas virtuales se realiza con periodicidad quincenal.

Para la extracción de las copias de seguridad en cintas, para las bases de datos se realiza semanal y para las máquinas virtuales quincenal.

Para la copia de seguridad de las bases de datos de SIGEP existen los siguientes tiempos de retención por cada tarea programada:

Tabla 8. Tiempos de retención copias de respaldo

Tarea	Media pool	Frecuencia	Retención	Retención (días)
Oracle_DESA Oracle_SIGEP	Incremental diario	Permanente	Permanente	365
	Full Semanal			
	Full Mensual	Mensual	12 meses	365

Fuente: Función Pública-2017

[3] Función Pública, 18/09/2017. Políticas De Respaldo, Custodia Y Recuperación De La Información.

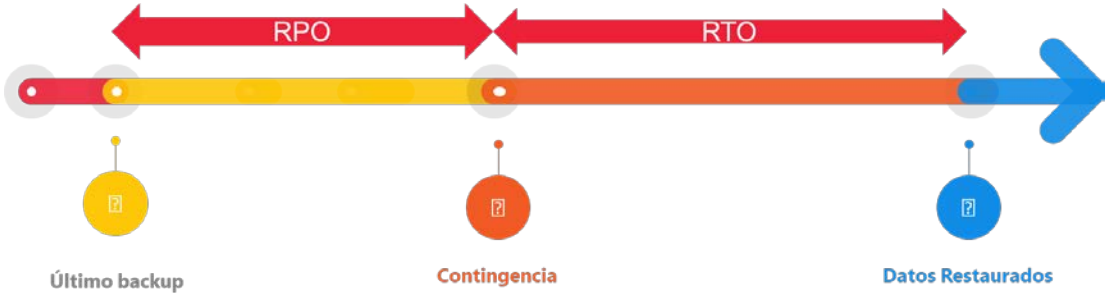
7. TIEMPOS RPO y RTO

RPO y RTO son conceptos fundamentales que en base a ellos se puede planificar y decidir qué tipo de soluciones son necesarias para el plan de continuidad de la Entidad.

RPO(Recovery Point Objetive - Punto Objetivo de Recuperación), punto en el tiempo a partir del cual los datos deben ser restaurados. Transacciones después de este tiempo deben ser capturadas a mano o a partir de los esquemas de contingencia. Esta es una definición general de lo que se denomina "pérdida aceptable" en una situación desastrosa.

RTO(Recovery Time Objetive -Tiempo objetivo de recuperación), lapso en el cual debe restaurarse el proceso después de un desastre.

Gráfica 7. Tiempos de recuperación de desastres



Fuente: CINTEL – 2017

RPO (Recovery Point Objective)

RPO se refiere al volumen de datos en riesgo de pérdida que la Entidad considera tolerable. Este depende de las Políticas de Respaldo, Custodia y Recuperación de la Información definida por la Entidad.

El RPO determina el objetivo de posible pérdida máxima de datos introducidos la última copia de respaldo, hasta la caída del sistema, y no depende del tiempo de recuperación.

A partir de las políticas de respaldo, custodia y recuperación de la información se establece que:

- RPO para las máquinas virtuales es de 15 días.
- RPO para las bases de datos es de 1 día.

7.1 RTO (Recovery Time Objective)

Expresa el tiempo durante el cual la Entidad puede tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

Pasos para seguir para recuperar las aplicaciones y los datos en caso de contingencia:

- Restaurar el servidor y su ambiente, sistema operativo. Dependiendo del tipo de problema pueden ser minutos, horas o días).
- Restaurar las copias de seguridad.
- Reanudar la operación.

Con relación al tiempo de restauración de la información se define que:

- RTO es de cuarenta y cuatro horas.

7.1.1 Proceso de Restauración

Se debe tener en cuenta los siguientes requerimientos:

1. Los líderes de proceso y jefes de dependencias son los únicos autorizados para solicitar la recuperación de información contenida en los servidores del centro de datos ubicado en la sede principal del Departamento Administrativo de la Función Pública. ante una pérdida total, parcial o para realizar pruebas controladas.

2. Se debe diligenciar en su totalidad el formato (Formato respaldo y Recuperación de Información) y ser entregado al administrador de copias.

3. Los tiempos previstos en los ANS con el servicio de custodia externa para la devolución de los medios magnéticos es de tres (3) horas después de recibida la solicitud de devolución.

4. Es responsabilidad del administrador de copias informar la disponibilidad de los respaldos, realizar el trámite para obtener los medios magnéticos, ejecutar el procedimiento de recuperación e informar los resultados.

5. Al finalizar el procedimiento se debe devolver el medio magnético solicitado en el proceso de restauración a la empresa de custodia.

8. RIESGOS Y VULNERABILIDADES

Se establecen los riesgos a los cuales están propensos los servicios de TI de la Función Pública, de igual manera determinar el nivel o factor de riesgo.

A partir del documento “SPI_Plan de tratamiento del riesgo” se identifican los riesgos que puedan afectar la continuidad del sistema de información SIGEP.

Tabla 9. Riesgos y vulnerabilidades

Amenaza	Vulnerabilidad	Riesgo	Escenario del Riesgo
Falla en activos de información	Calidad inferior de equipos (hardware)	Pérdida de disponibilidad de la información. Pérdida de la continuidad de las operaciones del negocio.	La disponibilidad del sistema de información SIGEP se puede verse comprometida debido a las vulnerabilidades y bajo desempeño presente en los equipos
Falla en activos de información	Exposición de los sistemas e Información crítica debido a vulnerabilidades técnicas de seguridad	Un solo punto dentro de la arquitectura falla	La falta de redundancia en servidores de aplicaciones o bases de datos.

Fuente. Función Pública

9. ACTIVIDADES DEL PLAN DE CONTINGENCIA PARA SIGEP

Las actividades del plan de contingencia se dividen en tres etapas:

- **La activación y notificación -** La activación de la Plan de contingencia donde se produce la simulación de una interrupción o corte que puede extenderse razonablemente más allá de la RTO establecido para el sistema.

- **Fase de Recuperación.** comprende las actividades de recuperación de las actividades para la recuperación del sistema afectado. Esta fase incluye las notificaciones y escalamiento para la recuperación.

- **Restauración.** Define las acciones tomadas para probar y validar la capacidad y funcionalidad del sistema en el punto original.

La desactivación incluye actividades para notificar a los usuarios de sistema de estado de funcionamiento. Esta fase también se ocupa de la recuperación de documentación esfuerzo, la finalización del registro de actividades, la incorporación de las lecciones aprendidas en las actualizaciones del plan, y los recursos prepara para cualquier evento futuro.

9.1 LA ACTIVACIÓN Y NOTIFICACIÓN

La activación y notificación define las medidas iniciales tomadas una vez el sistema presenta una interrupción que ha sido detectada o que parece ser inminente.

El plan de contingencia puede ser activado si uno o más de los siguientes criterios se cumplen:

1. El tipo de interrupción indica será mayor al establecido en el ANS del sistema de información
2. El elemento tecnológico afectado está dañado y puede no estar disponible dentro del tiempo establecido en el ANS

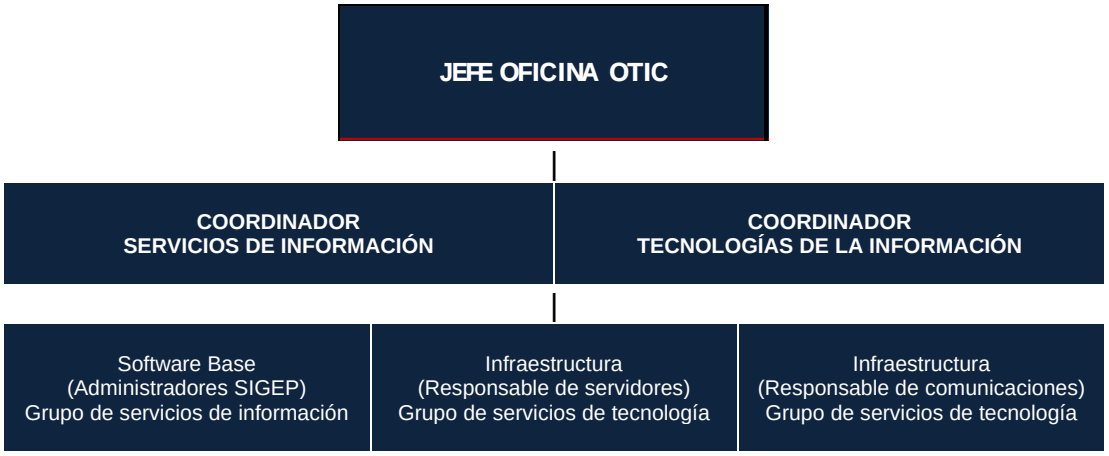
Para la activación de la contingencia se parte de los siguientes supuestos:

- Las copias de seguridad actuales del sistema de información y los datos están intactos y disponibles.
- Se ha identificado infraestructura para la contingencia.
- La indisponibilidad se genera en el ambiente de producción del sistema de información SIGEP.
- La afectación simulada consiste en una falla de la base de datos del ambiente de producción del sistema de información SIGEP.
- Se establece que, para el plan de contingencia, no se completa una contingencia para la información de anexos que hacen parte del sistema de información SIGEP. Por lo cual se debe contemplar la inactivación de las funcionalidades que afectan estos objetos. No funcionará la consulta ni la edición.

- El servicio de tareas programadas estará excluido del presente plan de contingencia. Esto afecta el proceso de cierre de contratos y la interoperabilidad con el servicio de distrito (SIDEAP).

Árbol de comunicación de activación del plan de contingencia es:

Gráfica 8. Árbol de comunicaciones del plan de contingencia



Fuente: CINTEL-2017

El primer paso después de la activación del Plan de contingencia es la notificación a los usuarios afectados:

- Clientes internos: Dirección de empleo público, Grupo de gestión humana, Oficina de comunicaciones, Grupo del servicio al ciudadano - SIGEP.
- Clientes externos: Entidades públicas, con sus servidores públicos y contratistas.

Publicación de banner de notificación de indisponibilidad del sistema de información, esto toma un tiempo aproximado de dos horas, esta actividad se desarrolla en paralelo a las actividades descritas en la siguiente tabla.

Las actividades en esta etapa son:

Tabla 10. Actividades para fase de activación y notificación del plan de contingencia

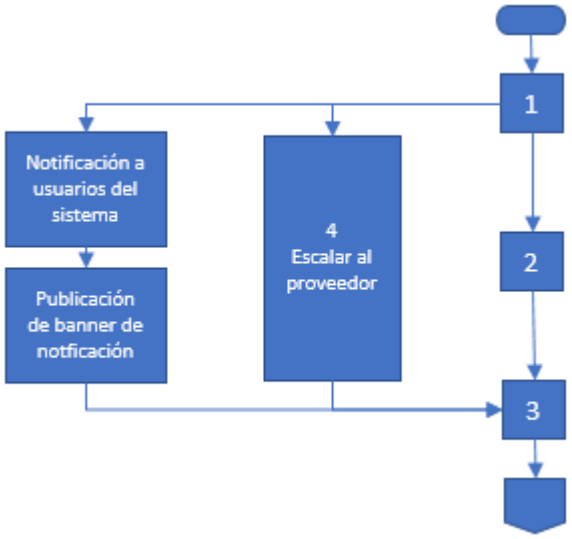
FASE		ACTIVIDAD	ROL RESPONSABLE	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS

Fase de Activación y notificación	1	Notificar la indisponibilidad y la activación del plan de contingencia.	Coordinador Sistemas de información	120
	2	Activar el plan de contingencia en la herramienta de mesa de servicio el cual habilita a los responsables la función de registro de las actividades	Administrador herramienta de mesa de servicio	30
	3	Realizar solicitud de copias de seguridad de bases de datos y de servidor de aplicación	Coordinador Sistemas de información	180
	4	Inactivar componente de anexos*	Coordinador Sistemas de información	360

*Acuerdo de ANS del plan contingencia con el proveedor.

Fuente: CINTEL-2017

Gráfica 9. Secuencia de desarrollo de actividades



Fuente: CINTEL-2017

Las actividades de notificación y de escalamiento a terceros se deben realizar en paralelo, las demás actividades se desarrollan en orden secuencial.

El tiempo estimado para el desarrollo de actividades de esta fase es de cinco horas y treinta minutos.

9.1.1 Fase de recuperación

Esta fase inicia con las notificaciones al personal responsable de la recuperación a partir de la matriz de roles y responsabilidades.

Las actividades en esta etapa se muestran en la siguiente tabla.

Tabla 11. Actividades fase de recuperación plan de contingencia

FASE		ACTIVIDAD	ROL RESPONSABLE	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
Fase de Contingencia	1	Importar la copia de respaldo en el hardware establecido como contingencia	Responsable servidores	360
	2	Restaurar la copia de respaldo sobre Oracle	Responsable servidores	360
	3	Verificar la restauración y activar base de datos de contingencia	Responsable bases de datos	120
	4	Instalación de ajustes para la inactivación de los anexos	Coordinador sistema de información	120
	5	Configurar la aplicación del ambiente de capacitación para que consulte la base de datos de contingencia	Coordinador sistema de información	60
	6	Asignación de direccionamiento público al servidor de aplicaciones	Responsable de redes y comunicaciones	180
	7	Configurar dominio para el servidor de aplicaciones y configuración de Certificado de Seguridad.	Responsable de redes y comunicaciones. Responsable Servidores.	180
	8	Realización de pruebas de funcionalidad	Coordinador sistema de información	120
	9	Propagación de DNS	Responsable de redes y comunicaciones	360
	10	Activar el servicio para el usuario externo	Coordinador sistema de información	30
	11	Notificar a los usuarios la disponibilidad del sistema	Coordinador sistema de información	60

FASE	ACTIVIDAD	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
Fase de Contingencia	1	360
	2	360
	3	120
	4	120
	5	60
	6	180
	7	180
	8	120
	9	360
	10	30
	11	

Fuente: CINTEL-2017

La actividad once se realiza en paralelo desde la actividad nueve.

Estas actividades se desarrollan en orden secuencial. El tiempo estimado para el desarrollo de actividades de esta fase es de 31 horas y 30 minutos.

A partir de este punto se realizan las actividades para solucionar la falla generada que puede basarse en restauración de una copia de seguridad en el ambiente de producción hasta reemplazo de hardware afectado.

9.1.2 Fase de restauración del servicio

Comprende las actividades para retornar al ambiente de producción en sus condiciones originales una vez se resuelva la incidencia que generó la afectación. Esta fase se activa una vez las bases de datos, servidores físicos, canales de comunicaciones se encuentran en funcionamiento.

Las actividades en esta etapa se describen en la siguiente tabla.

Tabla 12. Actividades fase de restauración

FASE		ACTIVIDAD	ROL RESPONSABLE	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
Fase de preparación y notificación	1	Programar la ventana de Ejecución para volver al ambiente de producción	Coordinador Sistemas de información	30
	2	Inactivar el acceso al SIGEP	Coordinador Sistemas de información	60

FASE		ACTIVIDAD	ROL RESPONSABLE	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
	3	Registrar de las actividades realizadas en la herramienta de mesa de servicio	Responsables de actividades	30
	4	Realizar copias de seguridad de bases de datos y de servidor de aplicación	Responsable de servidores Responsable de bases de datos	180
	5	Solicitar la activación de funcionalidades de anexo al proveedor*	Coordinador Sistemas de información	120

FASE		ACTIVIDAD	ROL RESPONSABLE	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
Fase de restauración	1	Importar la copia de respaldo en el ambiente de producción	Responsable servidores	360
	2	Restaurar la copia de respaldo sobre ambiente de producción	Responsable servidores	360
	3	Verificar la restauración y activar base de datos de producción	Responsable bases de datos	120
	4	Configurar la aplicación en el ambiente de producción para que consulte la base de datos de producción	Coordinador sistema de información	60
	5	Activación de los anexos	Coordinador sistema de información	120
		Activar las tareas programadas de SIGEP	Coordinador sistema de información	120
	6	Asignación de direccionamiento público al servidor de aplicaciones	Responsable de redes y comunicaciones	180
	7	Configurar dominio para el servidor de aplicaciones	Responsable de redes y comunicaciones	180
	8	Realización de pruebas de funcionalidad	Coordinador sistema de información	120
	9	Propagación de DNS	Responsable de redes y comunicaciones	360
	10	Activar el servicio para el usuario externo	Coordinador sistema de información	30
	11	Notificar a los usuarios la disponibilidad del sistema	Coordinador sistema de información	60

*Acuerdo de ANS del plan contingencia con el proveedor.

FASE	ACTIVIDAD	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
Fase de preparación y notificación	1	30
	2	60
	3	30
	4	180
	5	
FASE	**ACTIVIDAD**	**TIEMPO ESTIMADO DEL ESFUERZO MINUTOS**
Fase de Contingencia	1	360
	2	360
	3	120
	4	120
	5	60
	6	180
	7	180
	8	120
	9	360
	10	30
	11	

Fuente: CINTEL-2017

Tan pronto como la recuperación termine, se debe actualizar y activar la política de respaldo para SIGEP.

10. FASE 3 y 4: VERIFICAR y MEJORA CONTINÚA

En estas fases se realiza la simulación del plan y se documentan los resultados obtenidos a partir de las actividades descritas en la fase anterior.

El resultado de esta fase es un documento (Anexo 1. plan de pruebas) donde se obtiene el tiempo real del desarrollo de cada actividad y observaciones aportadas por el responsable. El responsable de sistema de información verifica el tiempo estimado de desarrollo de las actividades en comparación con el tiempo de ejecución establecido en el plan de contingencia.

Durante la ejecución de la prueba del plan de contingencia se genera un registro del desarrollo de cada una de las actividades dentro del Anexo 2. Registro de pruebas, de las observaciones generadas y de las nuevas actividades en caso de que sea el caso.

La ejecución de las pruebas del plan de contingencia le aporta a cada responsable conocimiento y entendimiento de sus actividades y responsabilidades.

Durante la ejecución de las pruebas se generan observaciones a partir de los resultados de las actividades lo que conlleva mejoras en el plan y van enfocadas a:

- Diagramas y arquitecturas del sistema de información
- ANS
- Política de respaldo
- Actualización plan de contingencia (actividades, tiempos, responsables).

11. ANEXOS

En la siguiente tabla se relacionan los anexos del documento

N°	Nombre de Anexo	Contenido
1	Anexo1. Plan de pruebas	Plan de pruebas del plan de contingencia de SIGEP
2	Anexo 2. Registro de pruebas	Formato de registro de las actividades de la prueba del plan de contingencia

ANEXO 1. PLAN DE PRUEBAS

1. PLAN DE CONTINGENCIA DE SIGEP

La primera prueba del Plan de contingencia es el punto de referencia para seguir realizando pruebas que sean más estrictas posterior a la implementación de los servicios y procesos definidos como críticos en centro de datos alterno, con la finalidad de poder asegurar la capacidad de Continuidad de la entidad.

La ejecución de las pruebas del plan de contingencia le aporta a cada responsable conocimiento y entendimiento de sus actividades y responsabilidades.

La siguiente tabla muestra el tipo de pruebas y ejercicio recomendados y su respectiva valoración:

Tabla 1. Pruebas

Tipo de Prueba o Ejercicio	¿Qué es?	Beneficios	Desventajas
Lista de Verificación	Distribuye planes para revisión.	Asegura que el plan cubra todas las actividades.	No está dirigido hacia la eficacia.
Recorrido Estructurado	Mirada detallada de cada paso	Asegura que las actividades planificadas estén descritas correctamente	Valor bajo al probar las capacidades de respuesta
Simulación	Escenario para representar los procedimientos de recuperación	Sesión practica	Si los procesos son muy diferentes
Paralelo	Prueba total, procesamiento principal no es interrumpido	Asegura un alto nivel de confiabilidad sin interrumpir la operación normal	Costo elevado al involucrar gran cantidad de colaboradores.
Interrupción Total	Es desastre, es replicado al punto de interrumpir las operaciones normales.	Pruebas más confiables de los planes	Un alto nivel de riesgo

Fuente: CINTEL

El presente plan de contingencia contempla el tipo de prueba paralelo; con este tipo de prueba no hay interrupción del servicio en el ambiente de producción durante la ejecución de las pruebas. Las pruebas se realizan en paralelo mediante la utilización del ambiente de capacitación del sistema de información SIGEP.

Descripción de actividades a desarrollar en la prueba del plan de contingencia teniendo relación con las actividades descritas en el apartado anterior. Las pruebas se desarrollan a partir de la simulación de una falla en el servidor de aplicaciones y en la base de datos.

Tabla 2. Actividades para fase de activación de la prueba del plan de contingencia

FASE		ACTIVIDAD	ROL RESPONSABLE	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
Fase de Activación de la prueba	1	Programar la ventana de Ejecución del plan de contingencia.	Coordinador Sistemas de información	120
	2	Iniciar con el registro de las actividades en la herramienta de mesa de servicio para disparar las notificaciones a los responsables	Coordinador Sistemas de información	30
	3	Simular ambiente aislado el nodo 1 de la base de datos.	Responsable Bases de datos	15
	4	Simular ambiente aislado el nodo 2 de la base de datos.	Responsable bases de datos	15

Fuente: CINTEL-2017

El desarrollo de las pruebas inicia las notificaciones al personal responsable de la recuperación a partir de la matriz de roles y responsabilidades.

Las actividades en esta etapa se muestran en la siguiente tabla. El alcance de las pruebas del plan de contingencia no contempla la participación de proveedores.

Tabla 3. Actividades fase de recuperación plan de contingencia

FASE		ACTIVIDAD	ROL RESPONSABLE	TIEMPO ESTIMADO DEL ESFUERZO MINUTOS
Fase de Contingencia	1	Importar la copia de respaldo en el hardware establecido como contingencia	Responsable servidores	360
	2	Restaurar la copia de respaldo sobre Oracle	Responsable servidores	360
	3	Activar base de datos de contingencia	Responsable bases de datos	120
	4	Configurar la aplicación del ambiente de capacitación para que consulte la base de datos de contingencia	Coordinador sistema de información	30
	5	Asignación de direccionamiento al servidor de aplicaciones	Responsable de redes y comunicaciones	180
	6	Configurar dominio de pruebas para el servidor de aplicaciones de contingencia. Para la prueba no se genera un nuevo certificado de seguridad.	Responsable de redes y comunicaciones	180
	7	Realización de pruebas de funcionalidad	Coordinador sistema de información	120

Fuente: CINTEL-2017

2. DESARROLLO DE LAS PRUEBAS

Durante la ejecución de la prueba del plan de contingencia se genera un registro del desarrollo de cada una de las actividades, de las observaciones generadas y de las nuevas actividades en caso de que sea el caso.

Tabla 4. Registro de Actividades de prueba del plan de contingencia

ACTIVIDAD		TIEMPO ESTIMADO DEL ESFUERZO MINUTOS	TIEMPO MEDIDO DURANTE LA PREUBA	OBSERVACIONES DE LA ACTIVIDAD
Prueba de Contingencia	1	360	120	Se solicitó el lunes por la noche y se trajo el martes por la mañana
	2	360	410 + 540	10:20 AM - 5:10 PM Martes 9:39 AM Miercoles 11 – 6:00 AM Jueves 12

	3	120	540	Jueves 12 9:00 – 18:00 Lentitud del servidor, base de datos pesado (250 Gb)
	4	30	180	
	5	180		
	6	180		
	7	120		

Fuente: CINTEL-2017

Finalmente, se diligencia la línea de conclusión del resultado de la ejecución de la prueba donde quedan registradas las notas concluyentes obtenidas a partir de la ejecución de la prueba.