



Banco de la República
Colombia

Prueba Tecnológica General
Febrero de 2019 – Horario NO hábil
Resultados

FICHA TÉCNICA

NOMBRE DE LA PRUEBA	Prueba Tecnológica General
TIPO DE PRUEBA	Nodo Primario del Banco de la República
ACTIVACIÓN (Fecha y horas)	Sábado, 16 de febrero de 2018 8:25 a.m.
RETORNO (Fechas y horas)	Entre el sábado, 23 de febrero de 2018 a las 7:30 a.m. y el viernes, 1 de marzo de 2019 a las 5:45 a.m.
ORGANIZADOR	Banco de la República - Colombia Dirección General de Tecnología Departamento de Servicios de Tecnología Informática(DSTI)
USUARIOS	Intermediarios Financieros, Banco de la República
PARTICIPANTES	Intermediarios Financieros, Banco de la República
DURACIÓN DE LA PRUEBA	Entre 1 semana y 15 días
SERVICIOS EXTERNOS	Access Manager Autenticación fuerte Atención al ciudadano Antares Bus de Servicios CEDEC CENIT CUD DCV Gestión de identidades GTA Financiero GTA Bitácora PKI Portal Sebra y sus componentes SEN S3 SUBASTAS SUCED
OTROS SERVICIOS	Varios relacionados con la función del Banco de la República



*Banco de la República
Colombia*

**Prueba Tecnológica General
Febrero de 2019 – Horario NO hábil
Resultados**

ANTECEDENTES

La Dirección General de Tecnología realiza anualmente dos pruebas tecnológicas del Nodo Primario (ubicado en la Central de Efectivo) hacia el Nodo Secundario (ubicado en el Edificio Principal), donde la activación se hace fuera de horario hábil y dos en que la activación se hace en horario hábil. Se opera en el ambiente de contingencia aproximadamente una semana.

En cumplimiento con el cronograma de pruebas de contingencia tecnológicas del año 2019, se procedió a realizar la prueba en horario No Hábil.

OBJETIVOS

La realización de la Prueba Tecnológica General se realizó con el propósito de:

- **ENTRENAMIENTO A LOS EQUIPOS:** Entrenar y poner en operación el equipo tecnológico de reanudación, a fin de adquirir destreza en la ejecución de los procedimientos y en el manejo de crisis tecnológica para el escenario planteado en situaciones de estrés.
- **PROCEDIMIENTOS:** Verificar que los procedimientos de activación tecnológica sean claros y estén completos. Igualmente, validar que los recursos utilizados para esta estrategia sean suficientes.
- **EJECUCIÓN CONJUNTA DE PROCEDIMIENTOS:** Verificar el comportamiento de los clusters¹ y de los distintos servicios al ser conmutados conjuntamente.
- **MEDICIÓN DE TIEMPOS:** Verificar el tiempo de conmutación automática de los clusters fuera de horario hábil y de la desconexión lógica de máquinas, así como la ejecución de los procedimientos manuales.
- **AUTONOMÍA:** Verificar la autonomía del Nodo Secundario.
- **DOCUMENTACIÓN:** Verificar la aplicabilidad de la documentación.
- **VALIDACIÓN DE AMBIENTES:** Validar que los ambientes de contingencia de los servicios funcionan correctamente.

¹ Conjuntos o conglomerados de computadoras construidos mediante la utilización de hardware comunes y que se comportan como si fuesen una única computadora. <https://es.wikipedia.org/wiki/Cluster>



*Banco de la República
Colombia*

**Prueba Tecnológica General
Febrero de 2019 – Horario NO hábil
Resultados**

PLAN DE PRUEBA

ALCANCE

La prueba está programada para que tanto la activación como el retorno se realicen en días de horario no hábil, para que no tengan un alto impacto en los servicios que presta el Banco. Se estima un tiempo aproximado de una semana de permanencia de los servicios en contingencia.

TIEMPO ESTIMADO

El tiempo estimado de activación de los servicios críticos es entre 90 y 120 minutos.

El tiempo estimado de activación para los servicios internos es entre 90 y 240 minutos.

ACTIVACIÓN

El día sábado 16 de febrero de 2018, se llevó a cabo la prueba de contingencia general. Con ella se simula un escenario de pérdida o daño del Centro de Cómputo Primario a través de desconexiones lógicas y de ejecución de procedimientos manuales y automáticos; lo anterior, para conmutar todos los servicios hacia el Centro Cómputo Secundario ubicado en el edificio Principal del Banco de la República.

La conmutación de los servicios tomó un tiempo aproximado de 6 horas.

La prueba fue realizada en dos etapas, durante la primera se conmutaron los servicios externos o de misión crítica y en la segunda etapa se conmutaron los servicios internos. Se construyeron grupos de servicios teniendo en cuenta sus horarios críticos, los tipos de contingencias (automáticas, manuales) y los tiempos de ejecución de las mismas.

La activación en contingencia de los servicios se realizó fuera de horario hábil.

RETORNO

La ejecución de cada uno de los procedimientos se realizó fuera de horario hábil con el propósito de no impactar la funcionalidad de los sistemas contemplados durante esta prueba.

El retorno se inició el sábado 23 de febrero de 2018 y finalizó el jueves 28 de febrero en la noche

Tanto para la Activación como para el Retorno se programaron chequeos de los servicios con el fin de corroborar su adecuado funcionamiento luego de cada procedimiento ejecutado.



RESULTADOS

ACTIVACIÓN

- **Tiempos**

Teniendo en cuenta la hora general de inicio y finalización, los tiempos de activación para los servicios críticos estuvieron entre la 8:25 a.m. y las 12:16 p.m.

- **Ejecución procedimientos**

De manera general, la ejecución de todos los procedimientos permitió el correcto funcionamiento de los servicios.

Sin embargo, se presentaron las siguientes particularidades:

- CUD: Al realizar el chequeo del servicio el sistema arrojó el mensaje "Autenticacion S3 entrust (Passcode)". Se escaló al ingeniero de Seguridad quien revisó LOGs y al identificar errores fue necesario un reinicio de los servicios del Access Manager
- SEN. En la activación, se identificó un mensaje que requería la ejecución de un procedimiento que no estaba documentado; adicionalmente, se requería de una contraseña que no estaba custodiada en la herramienta prevista para eso. Fue necesario escalar los dos casos con los ingenieros expertos y fueron resueltos.
- SUCED. El procedimiento de activación contemplaba el reinicio de los dos servidores de aplicaciones del servicio, en este escenario hay un servidor que no está disponible por lo cual fue necesario ajustar el procedimiento.

- **Funcionalidad**

De manera general, los sistemas de información mostraron un adecuado funcionamiento durante su operación en contingencia. Sin embargo, se presentaron las siguientes particularidades durante la semana de operación:

- Bus de Servicios. Demora en respuesta del BUS al servicio de Perfiles S3. Se revisaron LOGs del sistema y después de un tiempo sin intervención, el desempeño del sistema se normalizó. Se creó un problema en la herramienta interna de gestión, para hacerle seguimiento y encontrar la causa raíz de este comportamiento.
- DCV. Error en la pantalla Aceptación de Términos. Se identificó que en el servidor de contingencia se encontraba un directorio temporal creado por el servidor de aplicaciones con una versión anterior de uno de los programas. Para dar solución se eliminó dicho directorio en el ambiente de contingencia y se reinició el servidor de aplicaciones.
- Subastas. Lentitud en el sistema. La lentitud fue causada por la demora en la respuesta del Bus de Servicios, después de un corto tiempo el sistema se normalizó.



Banco de la República
Colombia

Prueba Tecnológica General
Febrero de 2019 – Horario NO hábil
Resultados

RETORNO

- **Tiempos**

De manera general, los tiempos programados para el Retorno de cada uno de los grupos planeados se cumplieron adecuadamente.

- **Ejecución Procedimientos**

En general, la ejecución de todos los procedimientos permitió el correcto funcionamiento de los servicios luego del retorno a su ambiente de producción.

- **Funcionalidad**

Posterior al retorno, los servicios operaron satisfactoriamente.



*Banco de la República
Colombia*

**Prueba Tecnológica General
Febrero de 2019 – Horario NO hábil
Resultados**

CONCLUSIONES Y RESULTADOS

- La automatización de procedimientos de contingencias ha permitido disminuir el tiempo de conmutación de los servicios y disminuir el riesgo operativo asociado a una ejecución manual.
- Las pruebas individuales de un servicio son indispensables luego de su migración o de su actualización de plataforma. Ello permite ajustar los elementos inherentes a su operación, lo cual incluye monitoreo, procedimientos de contingencia, custodia de contraseñas en Bóveda, entre otros.
- Los equipos interdisciplinarios son fundamentales a la hora de diagnosticar y resolver los eventos e incidentes reportados durante la operación de los servicios. Entre sus miembros están: administradores, jefes de operación, directores, ingenieros líderes, ingenieros DBAs, ingenieros de Seguridad, fabricantes, proveedores ingenieros de soporte, entre otros.
- El tiempo que toma la ejecución de los procedimientos y el éxito de su ejecución dependen en alguna medida del/los ejecutor(es). Lo anterior, debido a la experiencia y conocimiento de quien ejecuta.

Agradecemos su valiosa colaboración en este ejercicio que nos permite afianzar los procedimientos y recursos de contingencia, así como minimizar la incertidumbre en un evento de crisis.