Gestión de Continuidad de Negocio

Departamento de
Gestión
de Riesgos y Procesos

Subgerencia de Riesgos

Departamento de
Servicios de
Tecnología
Informática

Dirección General de Tecnología

2019

Sistema de Gestión de Continuidad de Negocio

Sistema de Gestión de Continuidad de Negocio (SGCN) Elementos

Marco de Referencia
Objetivos

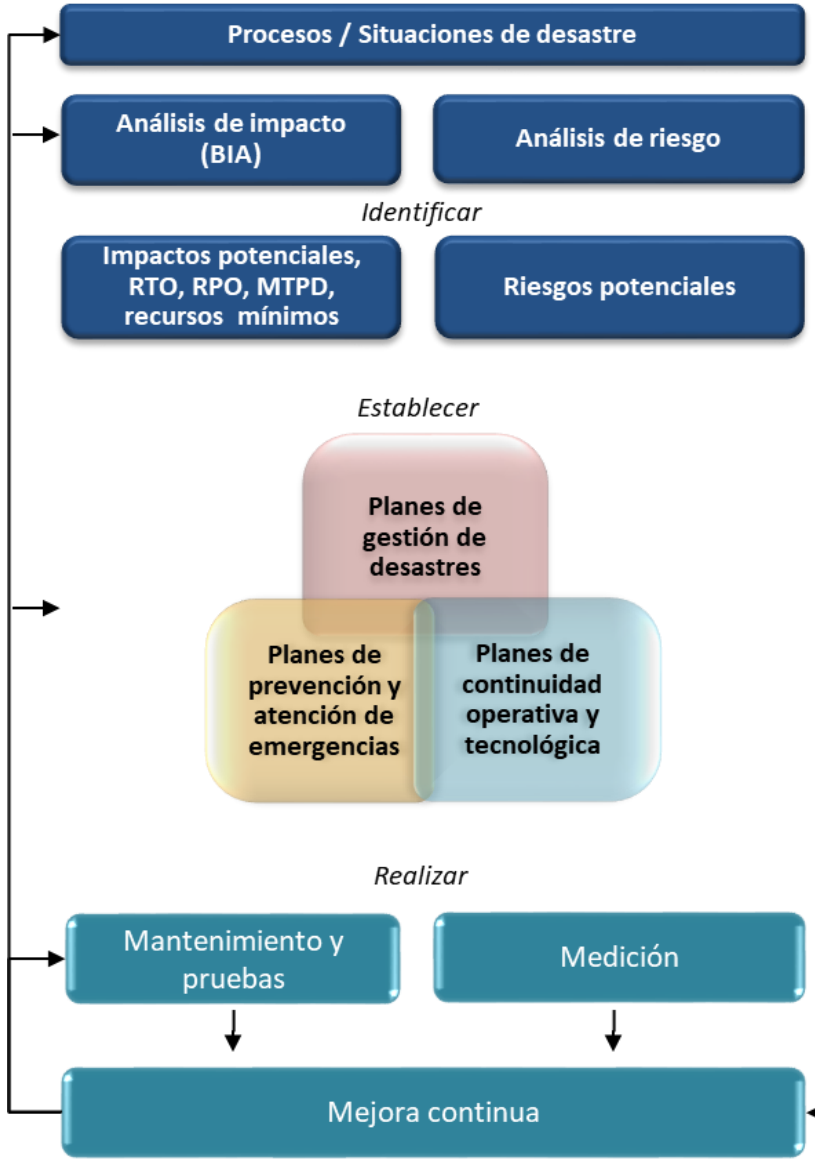
Objetivo General

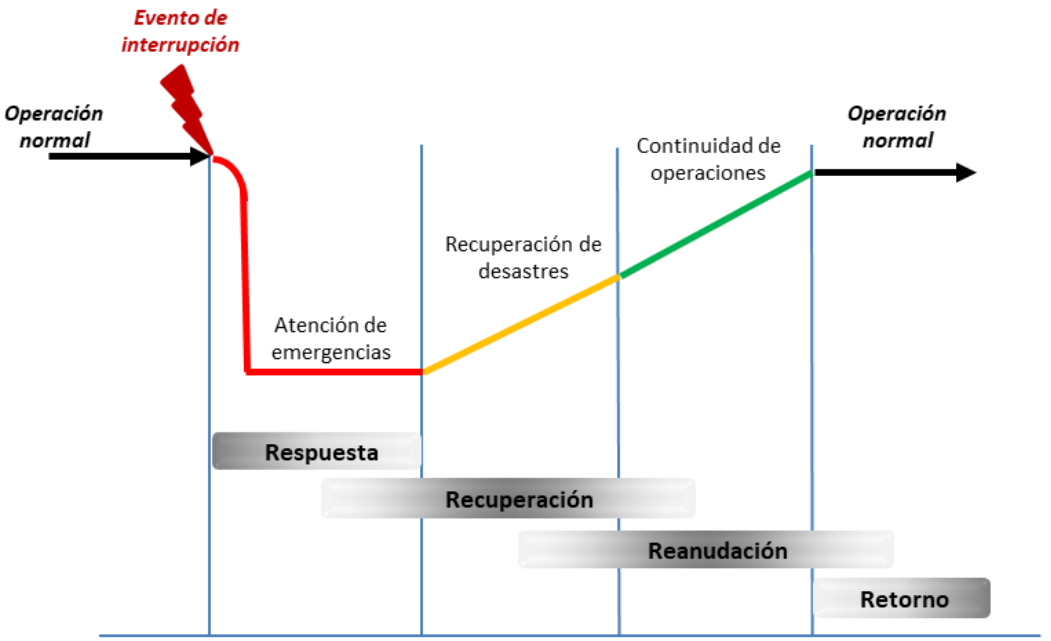
Fortalecer la capacidad del Banco para cumplir las funciones a su cargo ante situaciones que amenacen la continuidad de las mismas.

Objetivos Específicos

- Desarrollar planes de continuidad operativos y tecnológicos acordes a las metodologías establecidas por el SGCN, para los riesgos de interrupción identificados en los procesos críticos del Banco.
- Verificar que los planes de continuidad operativos y tecnológicos sean probados, evaluados y actualizados periódicamente.
- Comprobar de forma periódica que los recursos contingentes estén disponibles con el fin de garantizar su funcionamiento ante un evento real.
- Realizar el mejoramiento continuo del SGCN mediante el registro e implementación de acciones correctivas a partir de las mejoras identificadas.
- Desarrollar y probar planes de gestión de desastres para los procesos priorizados por la Alta Dirección, con sus correspondientes estrategias de negocio y de apoyo.

Modelo de Gestión de Continuidad





Procesos

Para realizar una gestión de continuidad adecuada, el BR ha desarrollado el **SGCN** conforme a los estándares de la norma ISO 22301:2012

El ciclo PHVA es el medio para asegurar que la continuidad del negocio esté siendo gestionada y mejorada eficazmente. Aplica para todas las partes del ciclo de vida de la gestión de la continuidad del negocio.

Plan de continuidad operativo

- **160 Estrategias Operativas**
  - Pruebas ejecutadas:
    - **2018:** 476
    - **2019:** 467*
  - No disponibilidad de recurso humano.
  - No acceso a edificaciones.
  - No disponibilidad de tecnología.
- **Estrategias de último nivel**
  - Envío y recepción de información por medios alternos.
  - Acceso remoto de empleados.
  - Apoyo a la operación desde sedes diferentes.

- **Centros Alternos de Operación**
  - Dos (2) CAO en Bogotá:
    - Ed. Anexo C (150 m. de Oficina Principal): 12 puestos de trabajo para procesos críticos.
    - Ed. Central de Efectivo (10 km. de Oficina Principal): 65 puestos de trabajo con capacidad de extenderse a dos salas adicionales de 30 puestos cada una.
  - Un (1) CAO en Barranquilla (900 km.):

  20 puestos de trabajo para procesos críticos.

*Cantidad de Pruebas ejecutadas a 30 de noviembre de 2019

Medición: Indicadores de Gestión

Cultura de continuidad	• Cumplimiento del plan de sensibilización. • Evaluación de capacitaciones.
Mejoramiento continuo	• Ejecución de acciones correctivas y de mejora. • Efectividad de las acciones correctivas y de mejora.
Disponibilidad de recursos	• Disponibilidad de recursos contingentes. • Impacto por no disponibilidad de recursos.
Pruebas inter-institucionales	• Cumplimiento del cronograma de pruebas con entidades externas. • Evaluación de pruebas con entidades externas. • Pruebas interinstitucionales fallidas/abortadas.
Cobertura de planes de continuidad	• Cobertura de escenarios. • Cumplimiento del cronograma de pruebas internas.

Medición Modelo de Madurez

Integración

- Entre planes operativos de las áreas
- Entre planes tecnológicos y operativos
- Entre planes tecnológicos y operativos

+

Planes de Atención Emergencias

+

Planes de Gestión de desastre

- **Sector Financiero**
  - Comité de Continuidad Asobancaria.
  - Comité Gestión de Crisis del Mercado de Valores.
  - Comité Infraestructuras Críticas – CCOC.
  - Ejercicios conjuntos (gestión de desastre).
- **Gobierno**
  - Asesorías en Gestión de Continuidad de Negocio y Gestión Desastre.
  - Intercambio de experiencias y conocimientos con Bancos Centrales internacionales.
  - Red de Seguridad del Sistema Financiero (Banrep, MHCP, Fogafin, SFC, URF).
- **Organismos de Emergencia**
  - Comunicación e Interacción.
  - Organismos Gubernamentales para Gestión de Riesgos y Atención de Emergencias: IDIGER, UNGRD, Bomberos, Policía, Of. Gestión de Riesgos en cada ciudad.

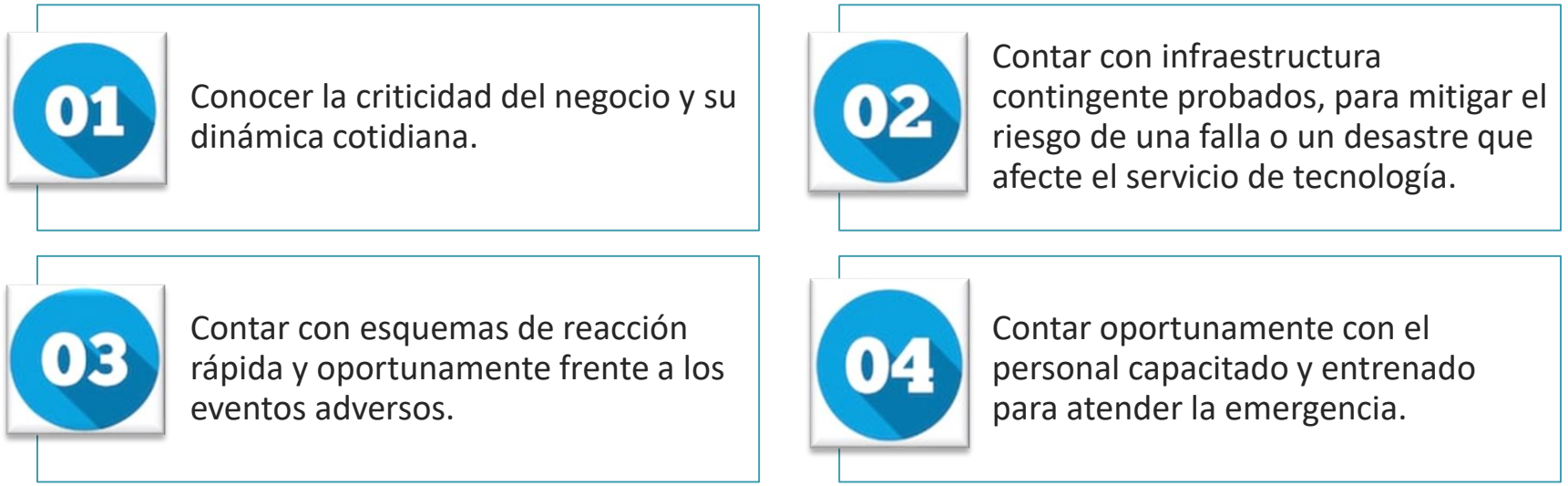
INTERNA

EXTERNA

Continuidad Informática y Tecnológica

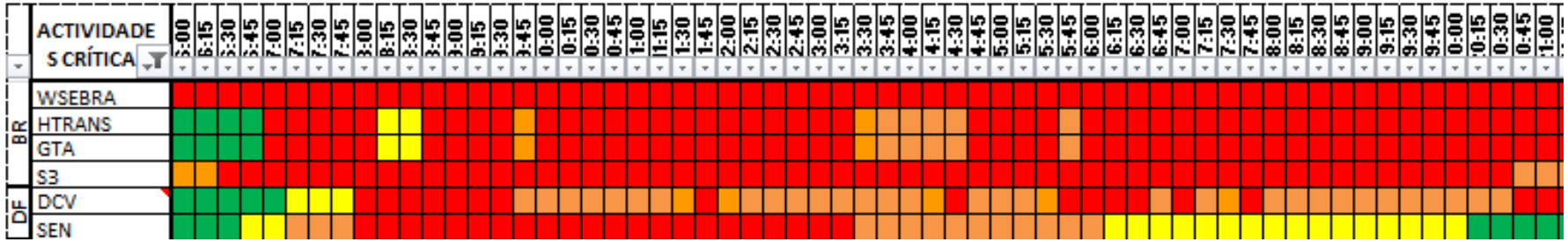
Contexto

- La operación del Banco de la República está fundamentalmente basada en servicios de tecnología.
- Factores claves para responder a eventos adversos contra la tecnología:



Requerimientos de Negocio

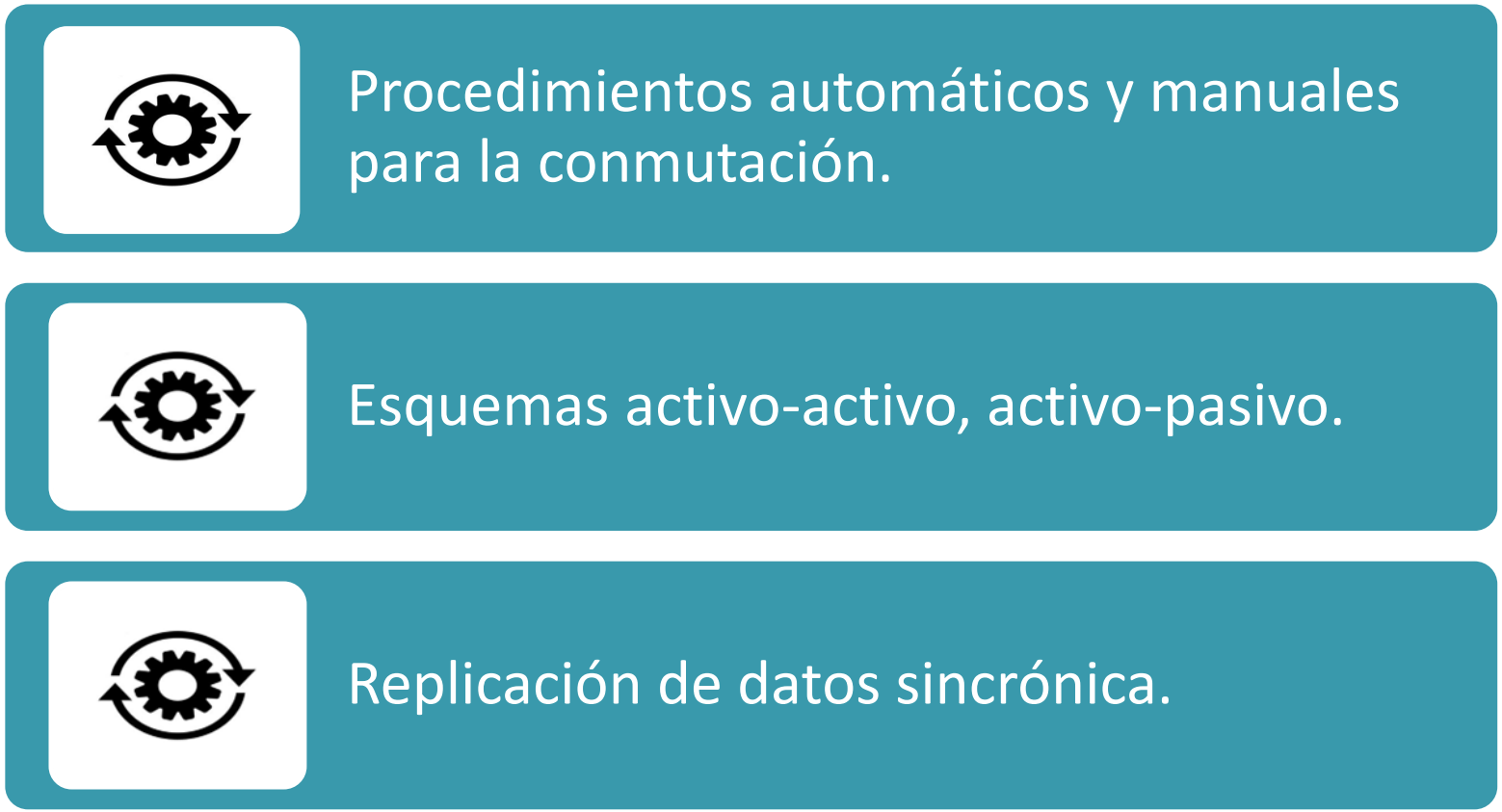
- Análisis de impacto → Priorización de los servicios de tecnología por criticidad para el negocio (BIA).
- Identificación de horarios críticos de los servicios.



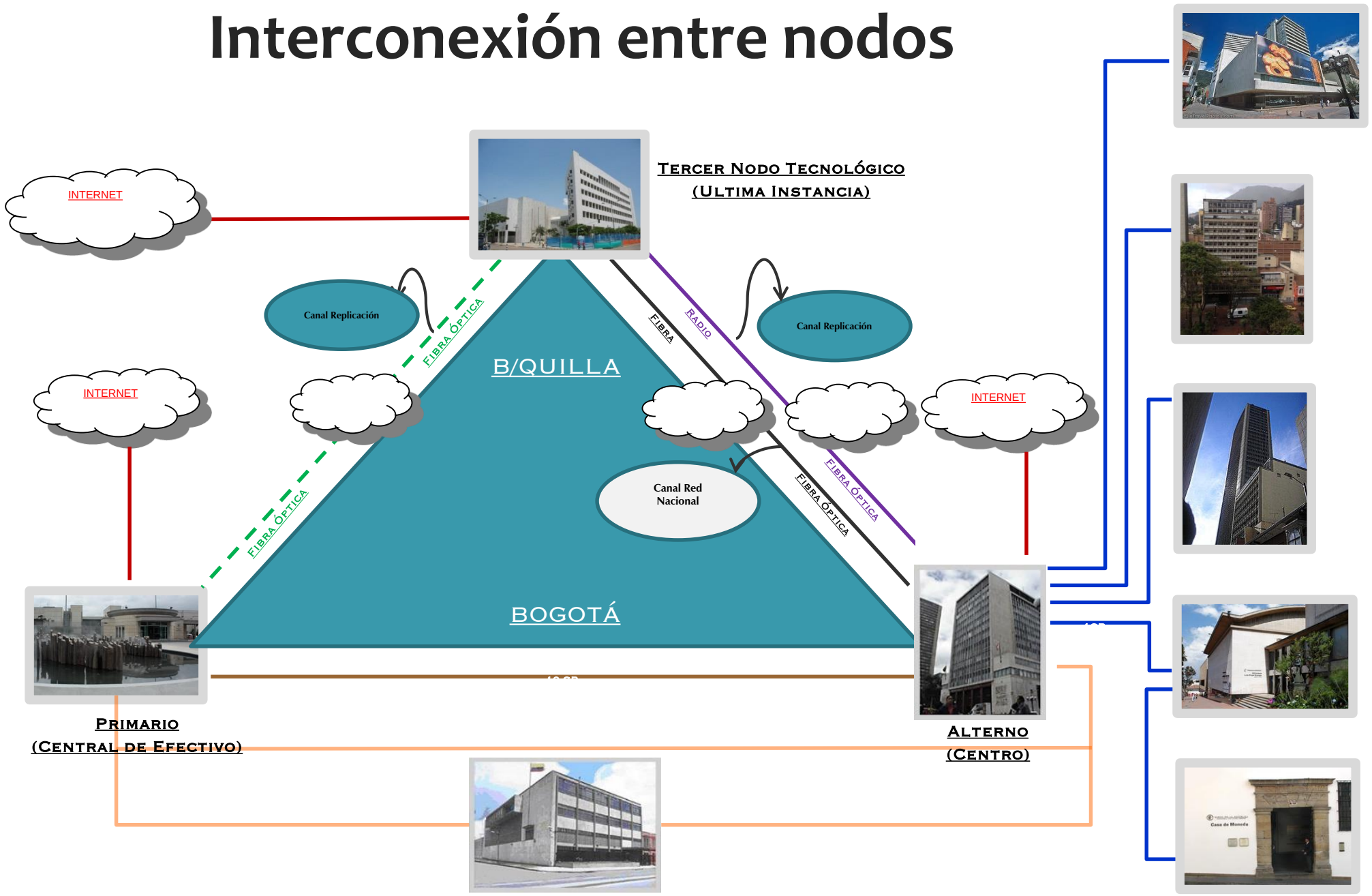
- RTOs y RPOs acordados con las áreas de negocio para cada servicio.
- Identificación de elementos tecnológicos críticos.
- Análisis de riesgos de los servicios tecnológicos.

Planes de continuidad tecnológica

- Servicios críticos sobre máquinas redundantes:



Interconexión entre nodos



Continuidad Tecnológica - Gestión de Desastres

- Agendas de control de desastres.
- Planes de contingencia (impresos en cada centro de cómputo).
- Herramienta de Automatización de procedimientos de contingencia (mallas).
- Equipos:
  - ✓ Equipo de reanudación.
  - ✓ Equipo de recuperación y apoyo.
  - ✓ Equipo de notificación.

Nodos Tecnológicos

Características del Nodo	Primario	Secundario	Tercer Nodo
Servicios	76 (26 Activo – Activo)	64	10
Tiempos de Reanudación	90 minutos – 240 minutos	90 minutos – 240 minutos	6-8 Horas
Procedimientos/ mallas durante Activación	13 / 22	19/16	20
Procedimientos durante Retorno	23/28	22/15	20

Planes de Continuidad Tecnológica

Centro de Procesamiento de Datos Alterno – Bogotá

Distancia: 15 km
Replicación total
RTO → 2 horas
RPO → 0 horas ~ On line (Sincrónico)
Estrategias: 82

Mecanismos de TI

Fibra Óptica
Clusters (Automático / Manual)
Replicación BD / SAN Storage
Balanceo de cargas

Centro de Procesamiento de Datos Alterno – Barranquilla

Distancia : 700 km
S.I Críticos y sus datos
RTO → 8 horas
RPO → 1 min – 8 días
Estrategias: 23

Mecanismos de TI

Enlace WAN
Replicación asincrónica
Envío de cintas semanal

Estrategias Tecnológicas

Servicio	App Server	RTO	Base de datos	RTO
DCV	Activo-Pasivo	15 minutos	Activo-Pasivo (cluster)	10 minutos
SEN	Activo-Pasivo	40 minutos	N/A	-
CUD	Activo-Activo	0 minutos	Activo-Pasivo (cluster)	10 minutos
CEDEC	Activo-Pasivo	20 minutos	Activo-Pasivo (cluster)	10 minutos
CENIT	Activo-Pasivo	20 minutos	Activo-Pasivo (cluster)	10 minutos
ANTARES	Activo-Pasivo	2 minutos	Activo-Pasivo (cluster)	10 minutos
S3	Activo-Activo	0 minutos	Activo-Pasivo (cluster)	10 minutos
WSEBRA	Activo-Activo	0 minutos	N/A	-

Pruebas de Continuidad Tecnológicas

- 4 pruebas por nodo programadas al año (2 en horario hábil y 2 en fin de semana).
- TNT (Tercer Nodo Tecnológico) Semanal para usuarios internos y 3 pruebas programadas al año con externos.
- Procedimientos tecnológicos individuales probados periódicamente (cambio de sistemas / paso a producción ~ 50 x año).
- Seguimiento a hallazgos.
- Equipos de reanudación y recuperación:
  - Recurso Humano: 2 Ing. infraestructura, 1 Ing. de soporte, 1 Ing. Telecomunicaciones, 1 Ing. de seguridad, 2 Ing. de continuidad, 2 técnicos centro de cómputo.

Gestión proactiva del servicio a través de la Gestión de Eventos

Con el fin de apoyar la eficiencia operativa de nuestros clientes, los servicios deben operar de manera adecuada dentro de los horarios de disponibilidad, en las condiciones de desempeño y calidad, seguridad, confiabilidad y continuidad establecidas para todos los servicios, para lo cual se debe llevar a cabo acciones de prevención de afectación a los usuarios mediante tareas proactivas como la gestión de eventos y soporte a los usuarios.

En caso de presentarse situaciones que afecten la correcta operación de los servicios se gestionan adecuadamente los incidentes y problemas, para recuperar la funcionalidad y el nivel establecido para cada servicio.

Gestión de Eventos a través de la realización de chequeos y monitoreo tempranos de la salud de los servicios.

Gestión de Eventos

Chequeo

- Validación manual, a través de la experiencia de usuario, de que un servicio se encuentre operando correctamente.

- Se ejecuta de manera temprana, antes de inicio de horario de operación de los servicios o después de un cambio en producción.
- Lo realizan personas del Centro de cómputo y Centro de Soporte.

Monitoreo

- Validación de la salud de un servicio a través de la verificación de que sus componentes estén operando correctamente (servidor, red, disco, CPU, memoria, procesos corriendo, web services, etc.)

- Ejecución permanente durante el horario del servicio.
- Personal de monitoreo, soporte y operación permanentes y dedicados para corregir de manera oportuna una falla.
- Puede contener acciones de ejecución automática para corregir una falla.

Sistema de Monitoreo

- Monitoreo de la experiencia del usuario final.
- Recursos avanzados de aislamiento de problemas.
- Dashboard basado en el usuario y en el rol el cual muestra el funcionamiento y el estado de los componentes de TI así como sus dependencias.
- Modelamiento de servicios críticos que incluye los componentes que lo conforman (incluyendo contingencias) relaciones con otros servicios, dependencias agregaciones, etc).
- Análisis de impacto en el servicio que permite establecer una correlación de eventos.