



Gestión de Continuidad de Negocio del Banrep

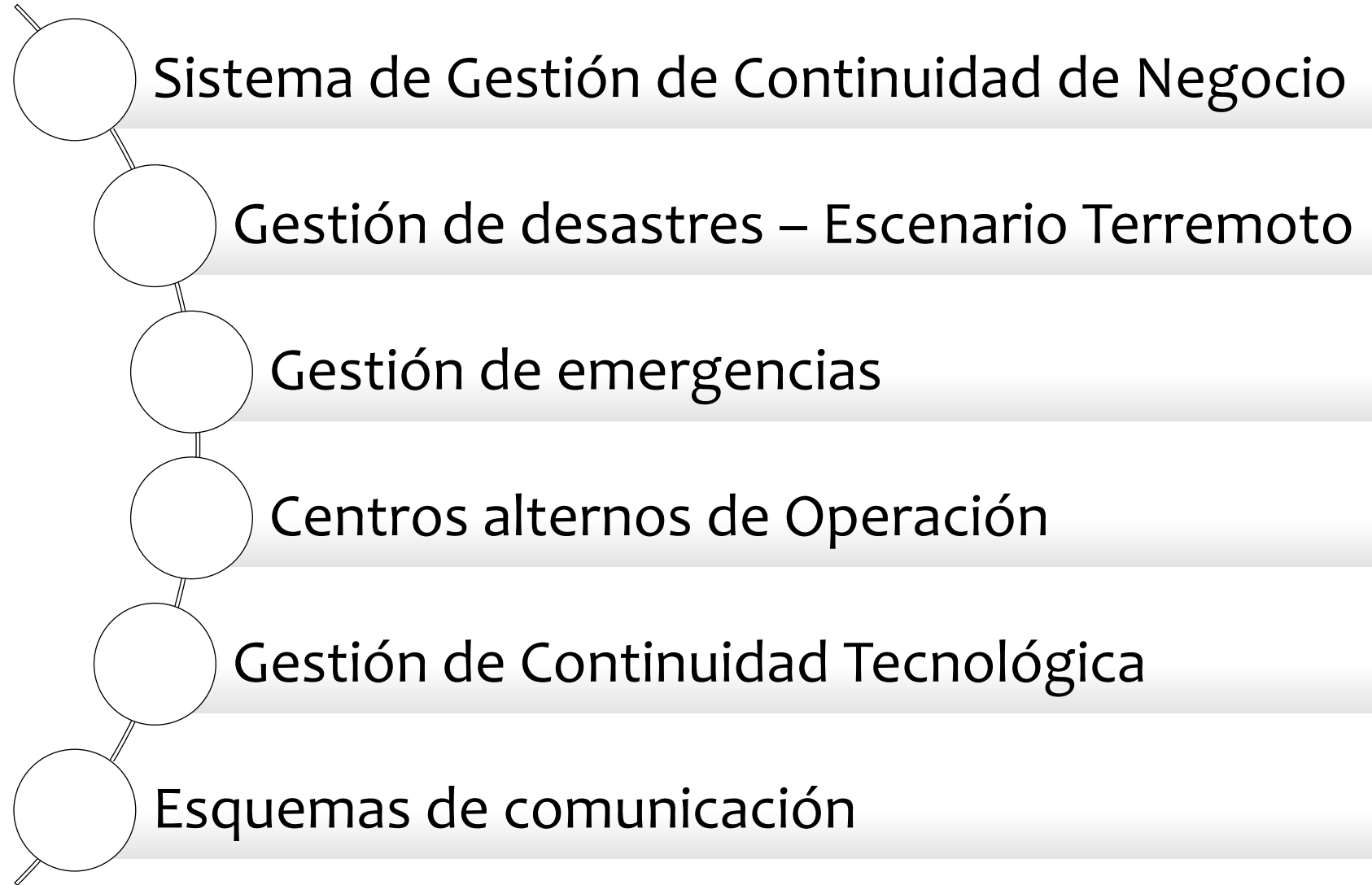
Departamento de Gestión de Riesgos y Procesos

Departamento de Servicios de Tecnología Informática

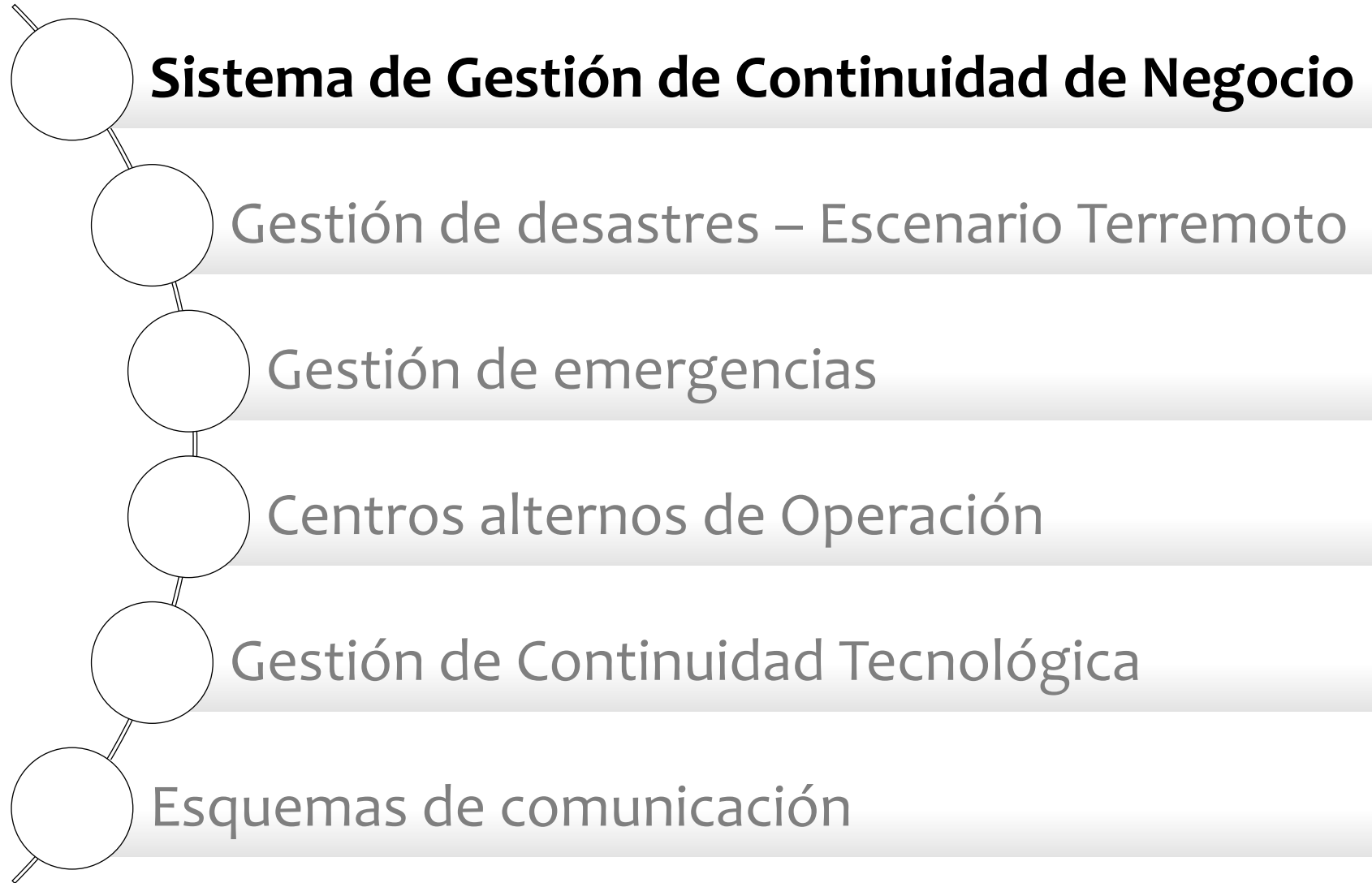
Departamento de Gestión de Salud

Julio 2025

Agenda



Agenda



Gestión de la Continuidad de Negocio 2024

En el último año se han realizado mejoras en el Sistema de Gestión de Continuidad de Negocio en los siguientes aspectos:



- > Actualización e implementación de la **metodología para la definición de los tiempos críticos de continuidad** (RTO, RPO y MTPD) para los procesos críticos del Banco.



- > Inclusión de **escenarios de ciberdesastre** en los protocolos de los procesos críticos.



- > Participación en proyectos especiales con un **esquema de continuidad de negocio** con el objetivo de mantener los procesos actualizados y administrar adecuadamente los riesgos operacionales asociados a la categoría de no disponibilidad.

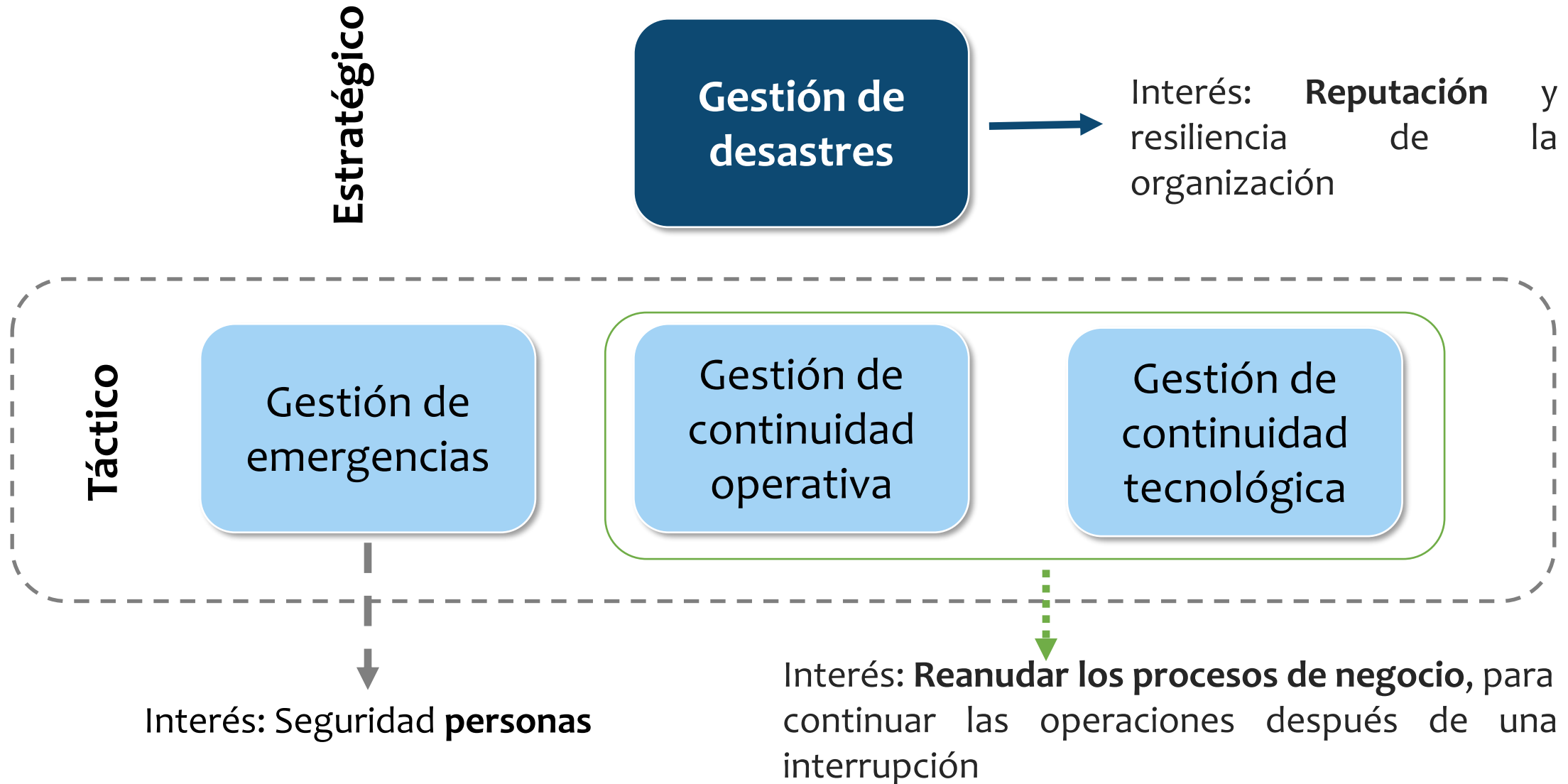


- > **Adquisición e implementación de una solución en la nube para administrar** los diferentes elementos del Sistema de Gestión de Continuidad de Negocio.

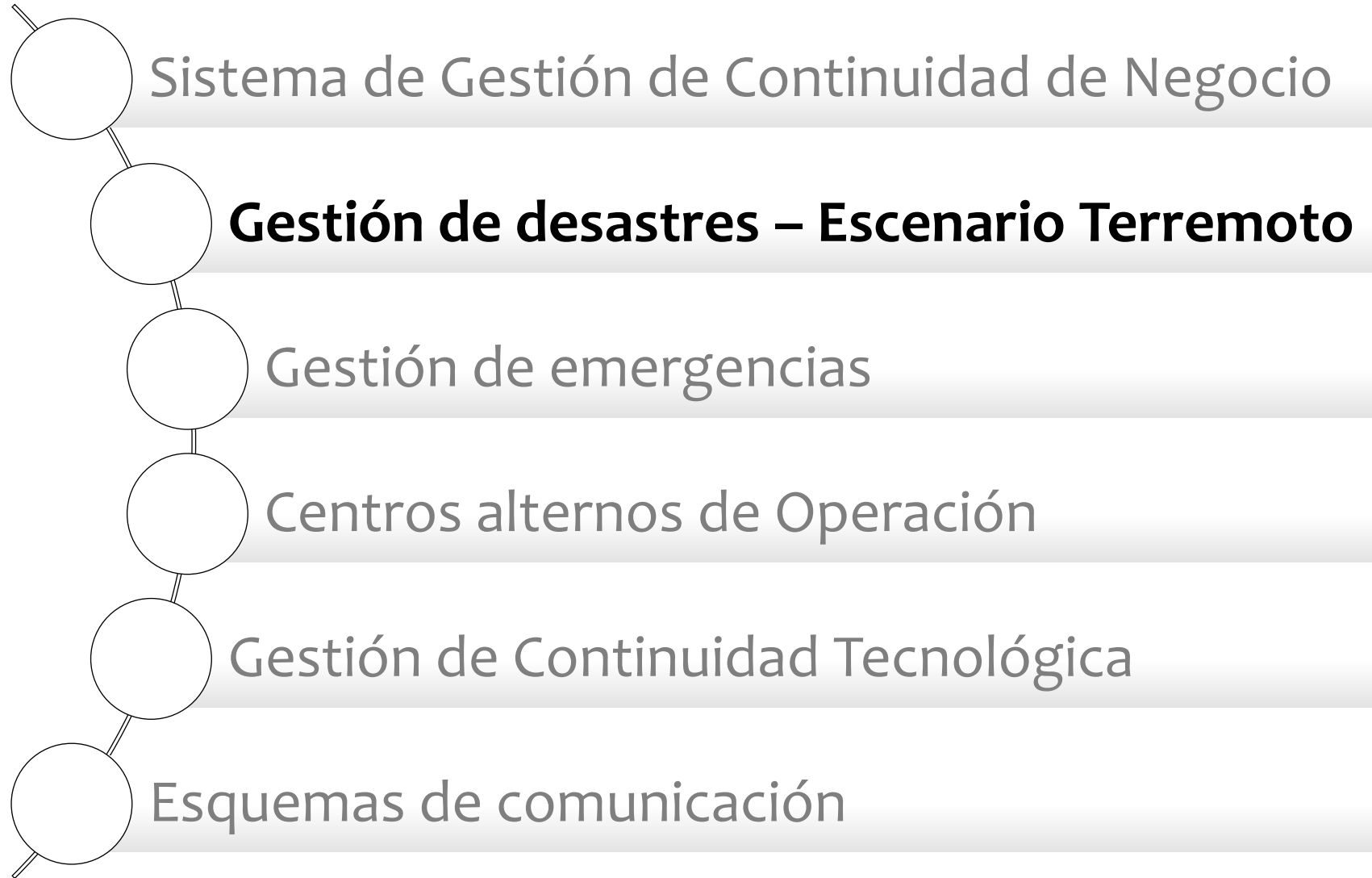


- > **TNT híbrido**

Gestión de la Continuidad de Negocio



Agenda



Gestión de Desastres: Principales componentes

Gobierno de gestión de desastres

Aprobado por el CA con respaldos, incluye estructura especial para desastres cibernéticos.

Salas de desastre

Sitios de reunión de los equipos de gobierno donde se mantiene el flujo de información sobre la evolución de los eventos y el control de la situación.

Ejercicios conjuntos

Con Bancos, transportadoras de valores y proveedores de infraestructura (protocolo de comunicaciones con la RSSF, protocolo de crisis del MVD).

Estrategias ante terremoto

En caso de terremoto en Bogotá se cuenta con **protocolos de gestión de desastre** y **23 planes de apoyo** (adquisiciones, transporte de valores, seguridad física, etc.).

Pruebas de conexión y del primer mecanismo de provisión de efectivo con entidades

Mecanismos de comunicación ante desastres

- > Teléfonos satelitales
- > Líneas de atención 018000
- > Portal de Información de Desastres (PID)
- > Sistema de notificación masiva



Protocolos de gestión de desastre

El BR ha venido **trabajando en diferentes protocolos** que le permiten prepararse para una adecuada actuación. A continuación, se presentan las **generalidades** de dichos protocolos:



Internos Banco de la República

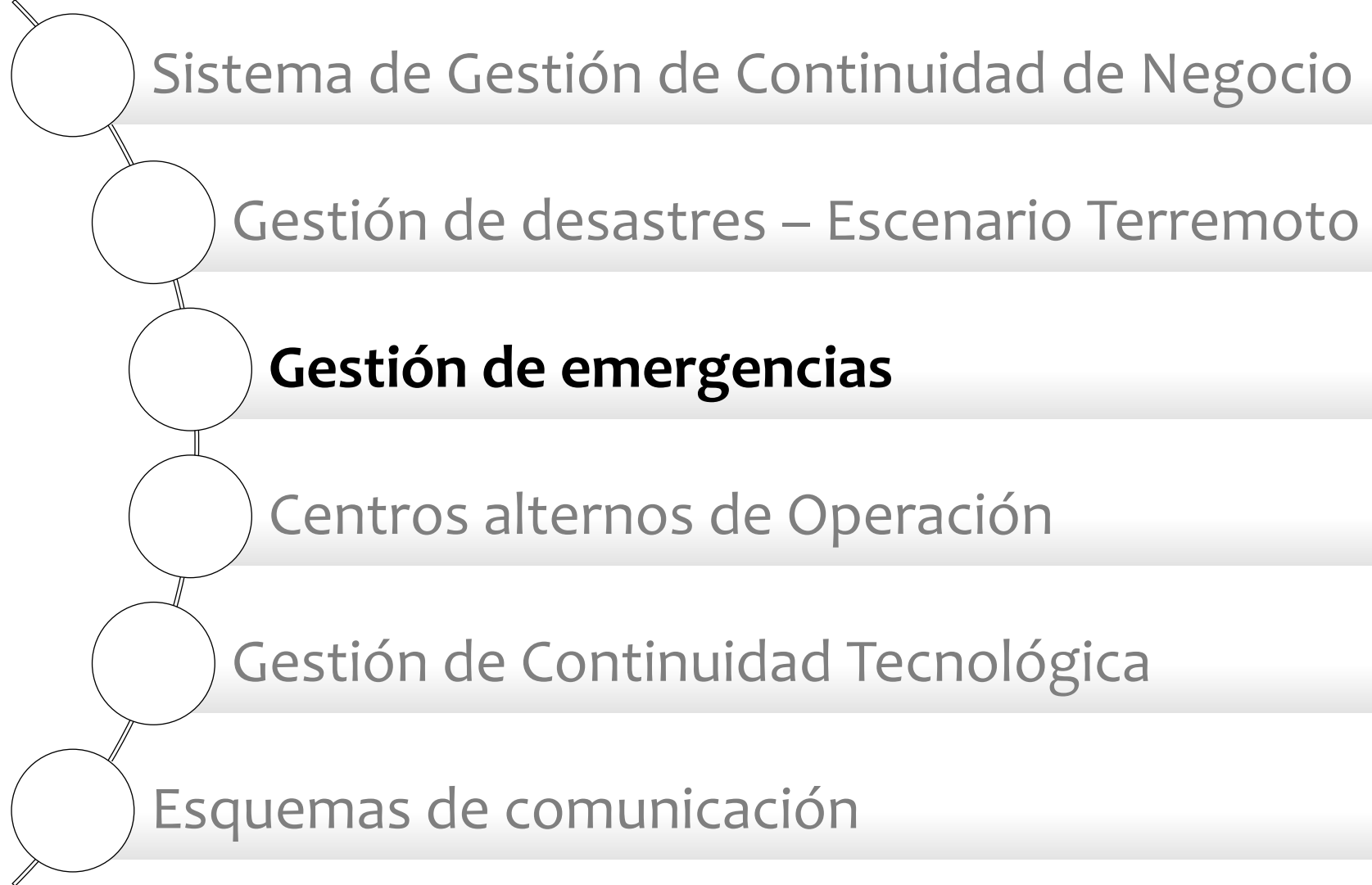
- > **Ciber desastres:** Establece procedimientos para reducir la probabilidad de interrupción y mitigar el impacto de la operación de los sistemas críticos¹ en eventos de fuga de información, denegación de servicio o malware.
- > **Provisión de efectivo:** Asegurar que la economía pueda hacer pagos a través del suministro de efectivo a entidades y ciudadanos . Pruebas semestrales
- > **Pagos de bajo valor – CENIT:** Prestar el servicio de pagos de bajo valor.
- > **Operaciones internacionales :** Cumplir los compromisos adquiridos y gestionar recursos de emergencia a través de la ejecución de operaciones internacionales del Gobierno.



Externos con sector financiero - Gobierno

- > **Mercado de valores y divisas:** Incluye reglas de operación y gobierno para proveedores de infraestructura ante eventos de desastre. Última prueba realizada: abril de 2022. **Regulado por la SFC en 2020 (CE 012 de 2018).**
- > **Asobancaria:** Incluye las estrategias y lineamientos a seguir por el gremio y las entidades financieras ante un evento de desastre que afecten el sector bancario y no de forma individual. **Finalizado en 2021.**

Agenda



Prevención y atención de emergencias: Principales componentes



Manuales

- > Manuales de prevención y atención de emergencias nacional y anexos del SPAE por edificación / estructura de gobierno.



Personas y capacitaciones

- > Brigadas básicas en cada uno de los edificios.
- > Brigadistas de atención de emergencia certificados.
- > Capacitaciones anuales.
- > Exámenes de aptitud por medio de valoración médica.



Simulacros

- > Dos (2) simulacros de evacuación anual por edificación



Análisis de vulnerabilidad

- > Diagnóstico de riesgo por amenazas y vulnerabilidades por edificación y desarrollo del plan de mejoramiento que se deriva del diagnóstico



Inspecciones

- > De seguridad industrial, de las aseguradoras del Banco, ARL y entes de control.



Tecnología aplicada

- > Sistemas de detección y extinción, así como, sistema de perifoneo en todas las edificaciones a nivel nacional.
- > Sistema de evacuación vertical en el edificio Anexo A y sucursal Buenaventura
- > Sistemas de altavoz en los edificios

Prevención y atención de emergencias

Esquemas de comunicación

- Radios en cada uno de los pisos en Bogotá y en sucursales distribuidos según necesidad.
- Megáfonos en áreas culturales
- Sistema de notificación masiva

Recursos de emergencia

- Botiquines
- Silla de evacuación por escaleras
- Desfibrilador externo automático
- Camillas

Infraestructura

- Plantas eléctricas con respaldos
- Revisión de redes eléctricas y puntos calientes
- Motobombas eléctricas con respaldo
- Sistemas de extinción

Otros recursos

- Contrato con Emermédica.
- Protocolos de almacenamiento de elementos de aseo y químicos, zonas de reciclaje, etc.
- En edificio principal y Fabrica de Moneda implementación del Plan Específico de Respuesta – PER con el cuerpo oficial de Bomberos

Elementos de seguridad

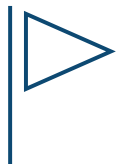
- Dotación para brigadistas de emergencia¹
- Paletas para las brigadas de evacuación
- Pasamanos
- Cintas antideslizantes
- Lámparas de emergencia
- Cintas fotoluminiscentes

¹. Casco, overol, gafas, botas y chalecos



Alerta telefónica, por mensaje de texto o correo electrónico

Permite **alertar a los empleados** cuando un evento de emergencia ocurra y solicitar su estado tras evacuar.



Eventos contemplados

Los eventos contemplados incluyen:

- Sismos
- Incendios
- Inundaciones
- Amenazas terroristas
- Manifestaciones violentas
- Pandemias

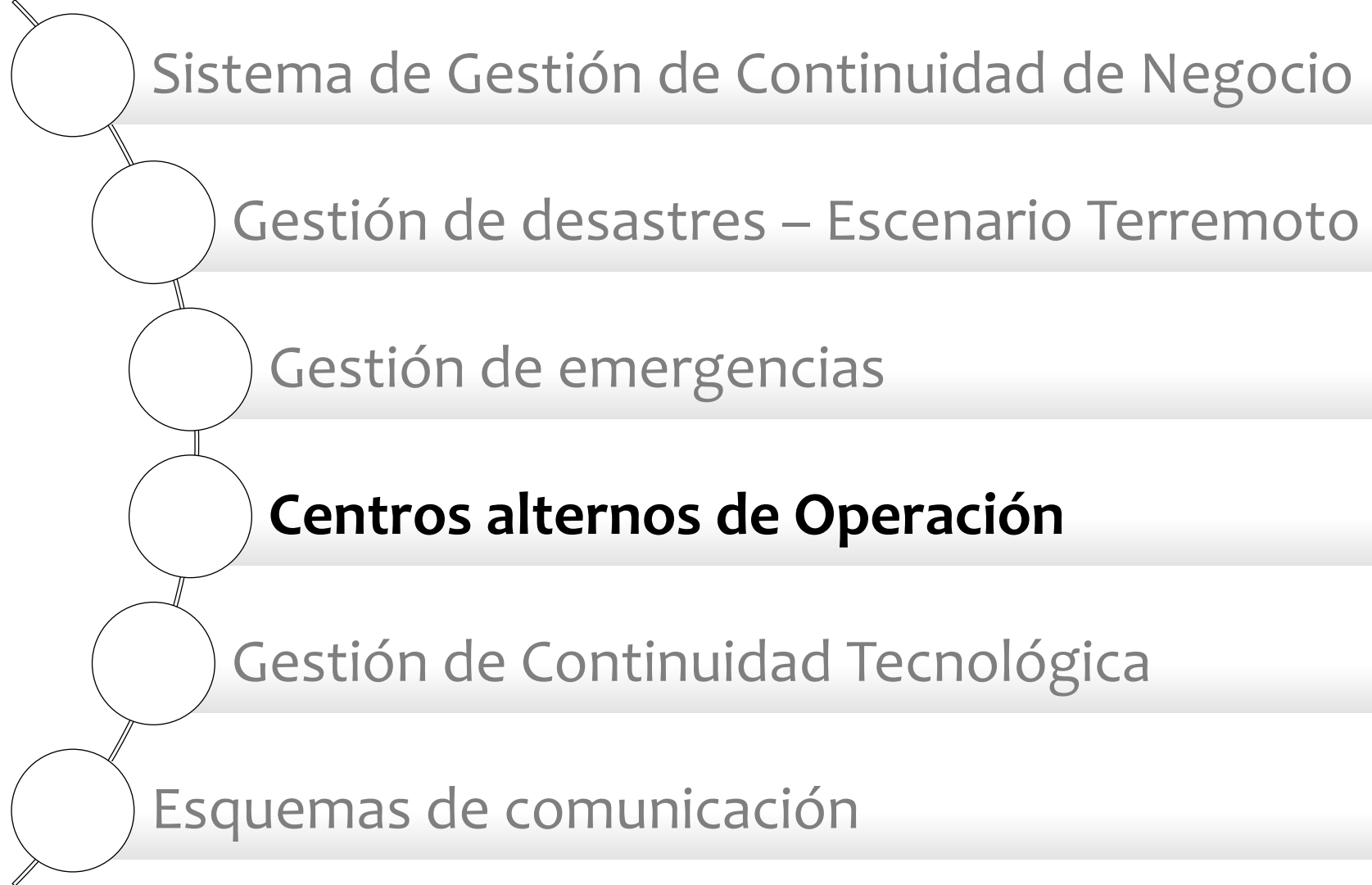


Personalización según tipo de evento

Cuenta con más de 80 plantillas de alertas configuradas para los eventos definidos.

1. Se ejecuta (1) prueba al sistema en cada simulacro de evacuación por edificio programado.

Agenda



Centros Alternos de Operación

Salas de contingencia: Espacios equipados para operar los procesos críticos en caso de eventos de acuerdo a los niveles de contingencia.



Edificio Anexo C

- > 150 m. de oficina principal
- > 12 puestos de trabajo
- > Se utiliza cuando el incidente no es generalizado y las operaciones no dan espera para el desplazamiento a la Central de Efectivo.



Central de Efectivo

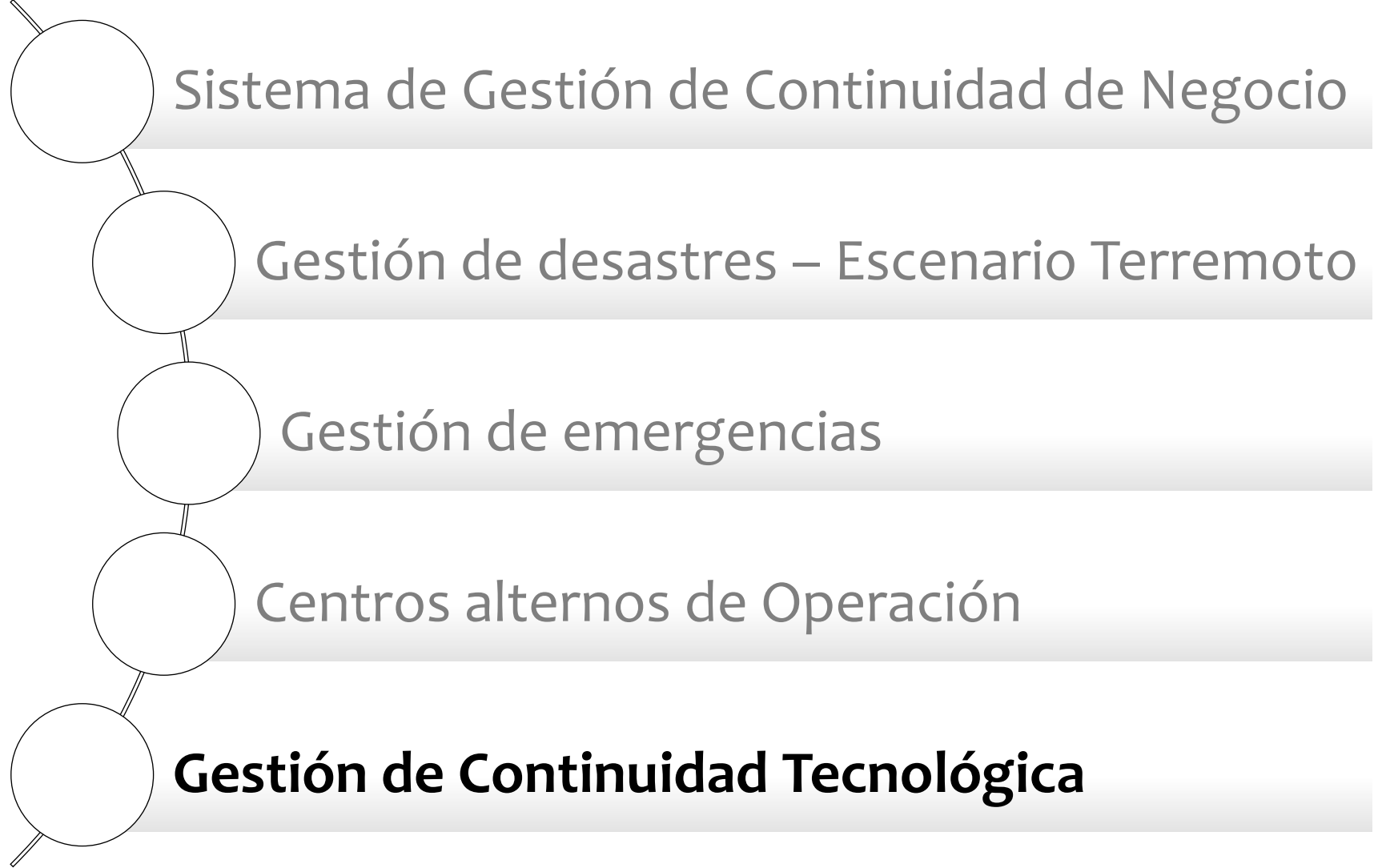
- > 10 km. de Oficina Principal.
- > 70 puestos de trabajo con capacidad de extenderse a dos salas adicionales de 30 puestos cada una.
- > Se utiliza en caso de que no haya acceso a las instalaciones del centro de Bogotá.



Sucursal Barranquilla

- > 900 km. De Oficina Principal
- > 20 puestos de trabajo.
- > Se utiliza en caso de que la ciudad de Bogotá quede completamente inhabilitada.

Agenda



Nodos tecnológicos



**Continuidad Tecnológica:
principales componentes**

- Dos (2) nodos (primario y secundario): primario en Bogotá (Central de Efectivo) y el secundario en Siberia - Cota ~ 17 km. aprox.
 - Activos los dos nodos, cada servicio Activo – Activo, o Activo-Pasivo según su arquitectura / replicación sincrónica
 - **RTO** = 2 horas para los servicios críticos
 - **RPO** = 0 (sin pérdida de información en los datos de los servicios)
-



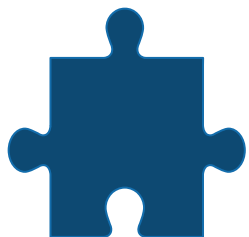
**Un (1) tercer nodo híbrido en
Barranquilla (aprox. 900
km.) para servicios críticos
de Banca Central**

- **RTO** = máximo 8 horas
- **RPO** = 1 min para procesos misionales que apoyan el proceso de provisión de efectivo entre 24 horas y 1 semana para otros procesos

Nota: Pruebas de nodo primario, secundario y tercer nodo según programación.



Pruebas de contingencia



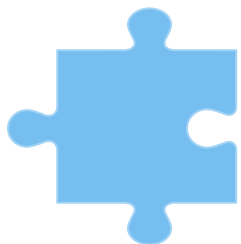
Prueba de Tercer Nodo Tecnológico

- **Alcance:** Suministro de efectivo ante eventos de desastres.
 - **Participantes:** Bancos, ACOS y Transportadoras de Valores.
 - **Frecuencia:** Trimestral.
-



Prueba de Nodo Secundario a Primario (horario hábil)

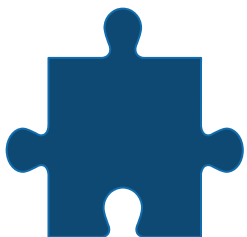
- **Alcance:** Simulación de pérdida del nodo secundario (edificio principal).
 - **Participantes:** Todas las entidades clientes del BR.
 - **Frecuencia:** Semestral.
-



Prueba de Nodo Secundario a Primario (horario NO hábil)

- **Alcance:** Simulación de pérdida del nodo secundario (edificio principal).
- **Participantes:** Todas las entidades clientes del BR.
- **Frecuencia:** Semestral.

Pruebas de contingencia¹



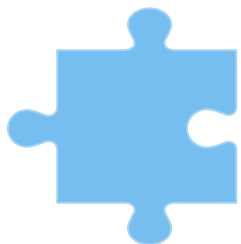
Prueba de Nodo Primario a Secundario (horario NO hábil)

- **Alcance:** simulación de pérdida del nodo primario (Central de Efectivo)
 - **Participantes:** Todas las entidades clientes del BR
 - **Frecuencia:** Semestral
-



Pruebas individuales de servicios (horario hábil o no hábil)

- **Alcance:** Poder probar la contingencia de un servicio después de algún cambio
 - **Participantes:** Todas las entidades clientes del BR
 - **Frecuencia:** De acuerdo a las necesidades de las entidades.
-

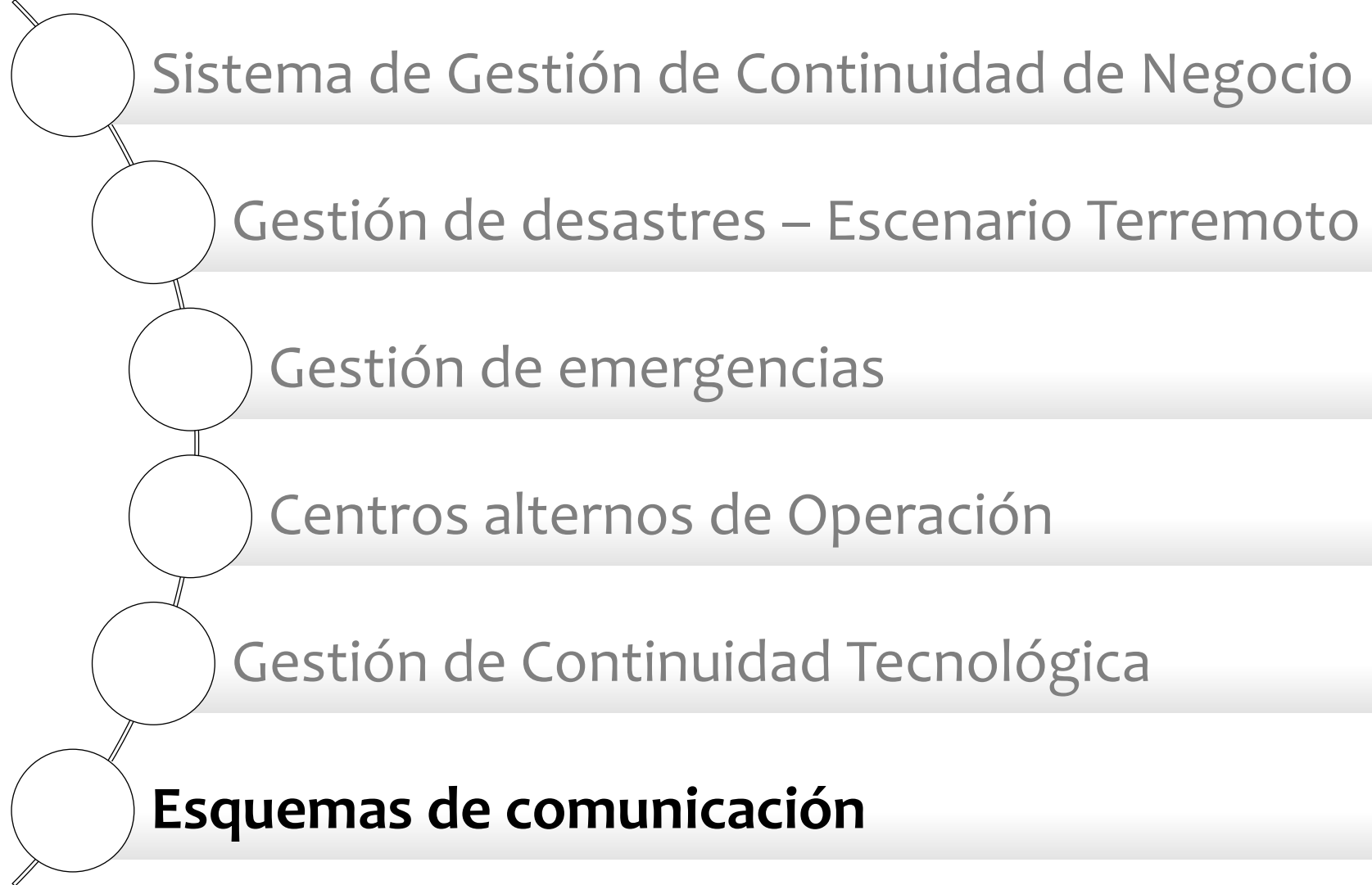


Prueba de Nodo Primario a Secundario (horario hábil)

- **Alcance:** Simulación de pérdida del nodo primario (Central de Efectivo)
- **Participantes:** Todas las entidades clientes del BR
- **Frecuencia:** Semestral

1. En el siguiente enlace puede encontrar el cronograma de pruebas con mayor detalle: <http://www.banrep.gov.co/es/continuidad/pruebas-contingencia>

Agenda



Esquemas de comunicación de incidentes

- 1 Correo electrónico a cuentas ContinuidadBR@entidad indicando la no disponibilidad del servicio.
- 2 Mensaje en el sistema de audio-respuesta: 3431000 (línea de soporte).
- 3 Correo electrónico indicando que el servicio ya se encuentra disponibles y la hora de inicio y fin del incidente.



Esquemas de comunicación - Contingencias

- 1 Correo electrónico a cuentas **ContinuidadBR@entidad** indicando los **servicios** que se encuentran **en contingencia**.
- 2 Mensaje en el sistema de audio-respuesta (línea de soporte): (601) 484-9980 (**si es masivo**).
- 3 Correo electrónico indicando que el **servicio ya se encuentra disponible** y la hora de inicio y fin.

Estado de los servicios a través del sitio web BR (pruebas):
<http://www.banrep.gov.co/es/continuidad/estado-servicios>



Prueba de **contingencia** –

Horarios de corte de servicios externos

Cordial Saludo,

Buenastardes.

Con el fin de que las áreas operativas puedan proceder a realizar los ajustes de los horarios de los servicios externos, nos permitimos informar que los cortes de éstos durante la prueba de **contingencia** fueron los siguientes:

SERVICIO	HORA DE CORTE	HORA DE SUBIDA
ANTARES	1:35 PM	3:07 PM
CEDEC	1:35 PM	3:07 PM
CENIT	1:35 PM	3:07 PM
CUD	1:35 PM	3:07 PM
DCV	1:35 PM	3:07 PM
GTA FINANCIERO	1:35 PM	2:20 PM
PORTAL WSEBRA	1:35 PM	1:40 PM
S3	1:35 PM	3:07 PM
SEN	No tuvo indisponibilidad	
SUBASTAS	1:35 PM	3:07 PM
SUCED	2:55 PM	3:07 PM

Cordialmente,

Departamento de Servicios de Tecnología Informática
Dirección General de Tecnología

Esquemas de comunicación Cambios

- 1 Correo electrónico a cuentas **ContinuidadBR@entidad** indicando el **cambio que se realizará sobre el servicio**.
- 2 Si es necesario hacer algún cambio en el cliente.
- 3 **Si genera o no** indisponibilidad del servicio.
- 4 Si tienen dudas escribir o llamar.

**ASUNTOS TECNOLÓGICOS**

**Mantenimiento Balanceo de Aplicaciones**

Cordial Saludo,

Les informamos que el sábado **27 de marzo de 2021**, desde las 8 a.m. y hasta las 12:00 p.m., se llevará a cabo un mantenimiento programado sobre el servicio **Balanceo de Aplicaciones** del banco.

La actividad no requiere cambios en las estaciones cliente.

En caso de cualquier inquietud, les solicitamos escribir a la dirección de correo MesaDeAyuda@banrep.gov.co o contactar al Centro de Soporte Informático en la línea 3431000.

Atentamente,

Departamento de Servicios de Tecnología Informática
Dirección General de Tecnología

JPRC - Para radicar sus peticiones, quejas, reclamos, felicitaciones, sugerencias y denuncias de actos de corrupción pulse aquí.

Esquemas de comunicación - SFC

El **BR** informa a la **SFC** a la dirección de correo riesgooperativo@superfinanciera.gov.co, los **eventos** que afectan de manera **significativa** la **confidencialidad, integridad o disponibilidad** de la información manejada en los sistemas haciendo una breve descripción del incidente y su impacto.



¡Gracias!
