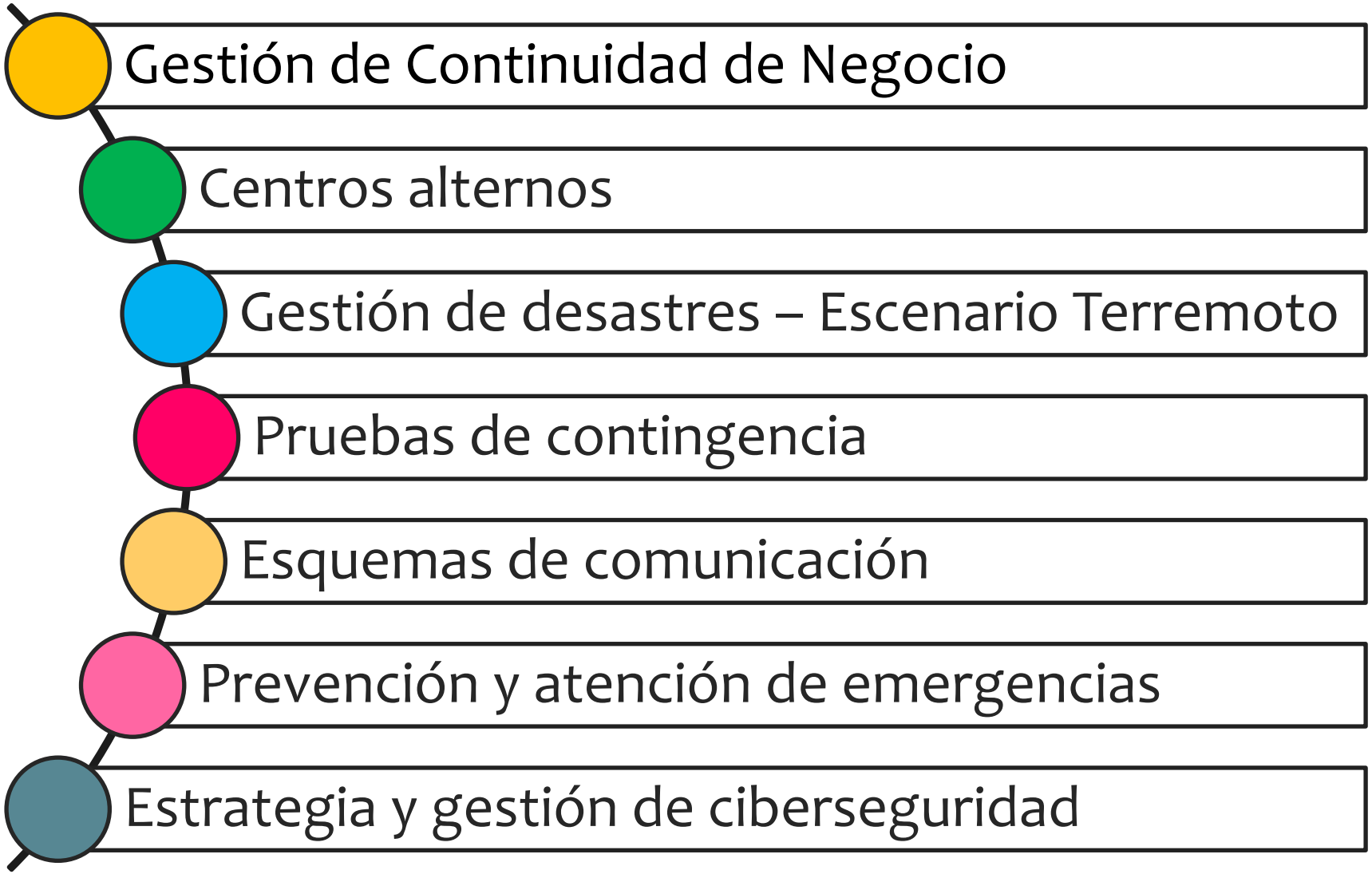
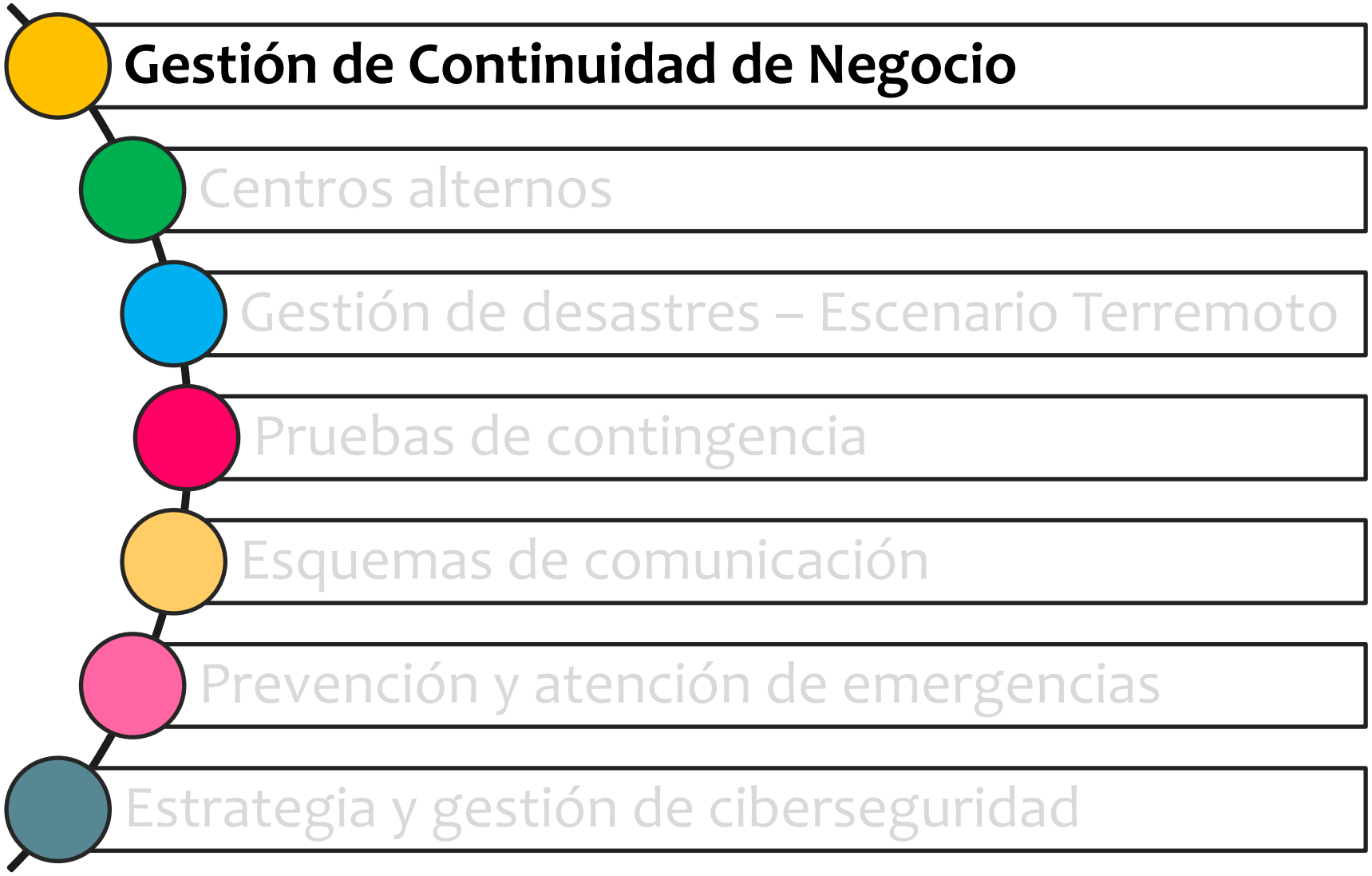
Gestión de Continuidad de Negocio del Banrep

Departamento de Gestión de Riesgos y Procesos
Departamento de Servicios de Tecnología Informática
Departamento de Seguridad Informática
Febrero 2022

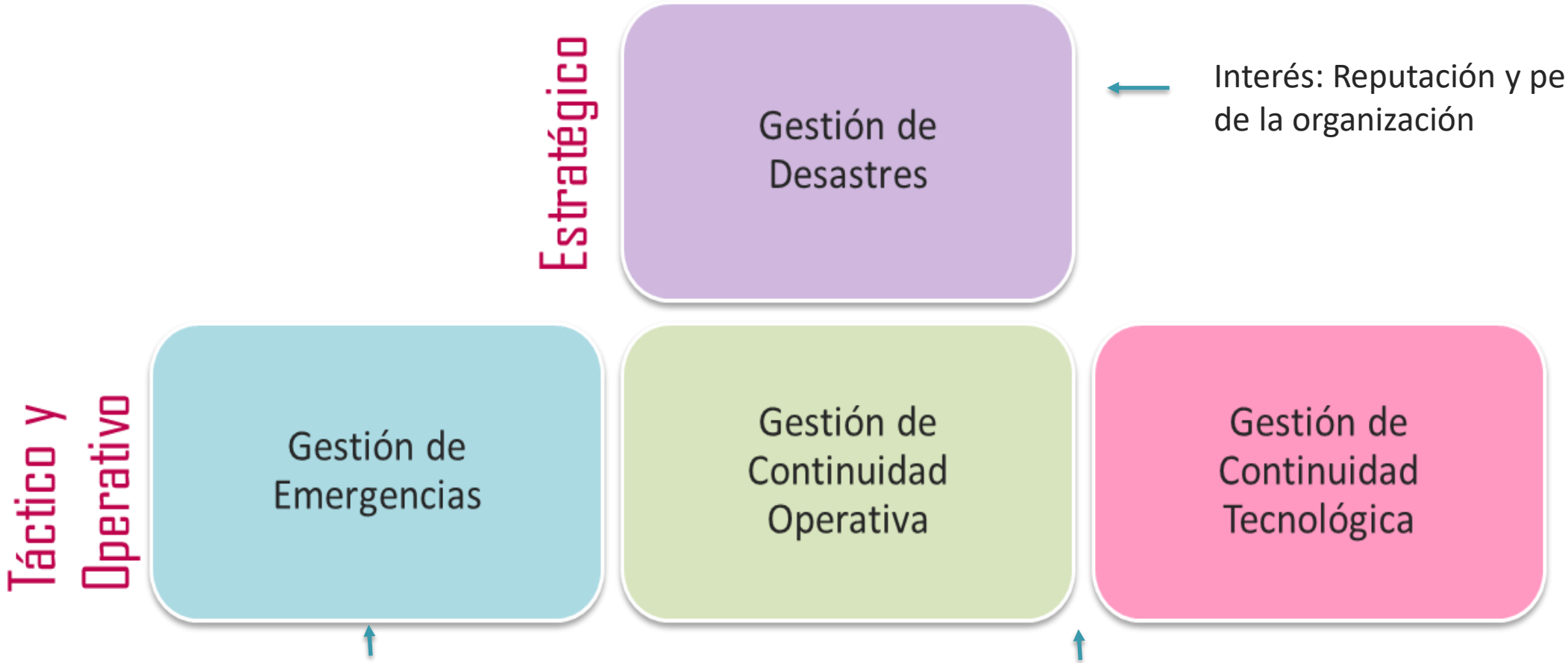
Agenda


Gestión de Continuidad de Negocio
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

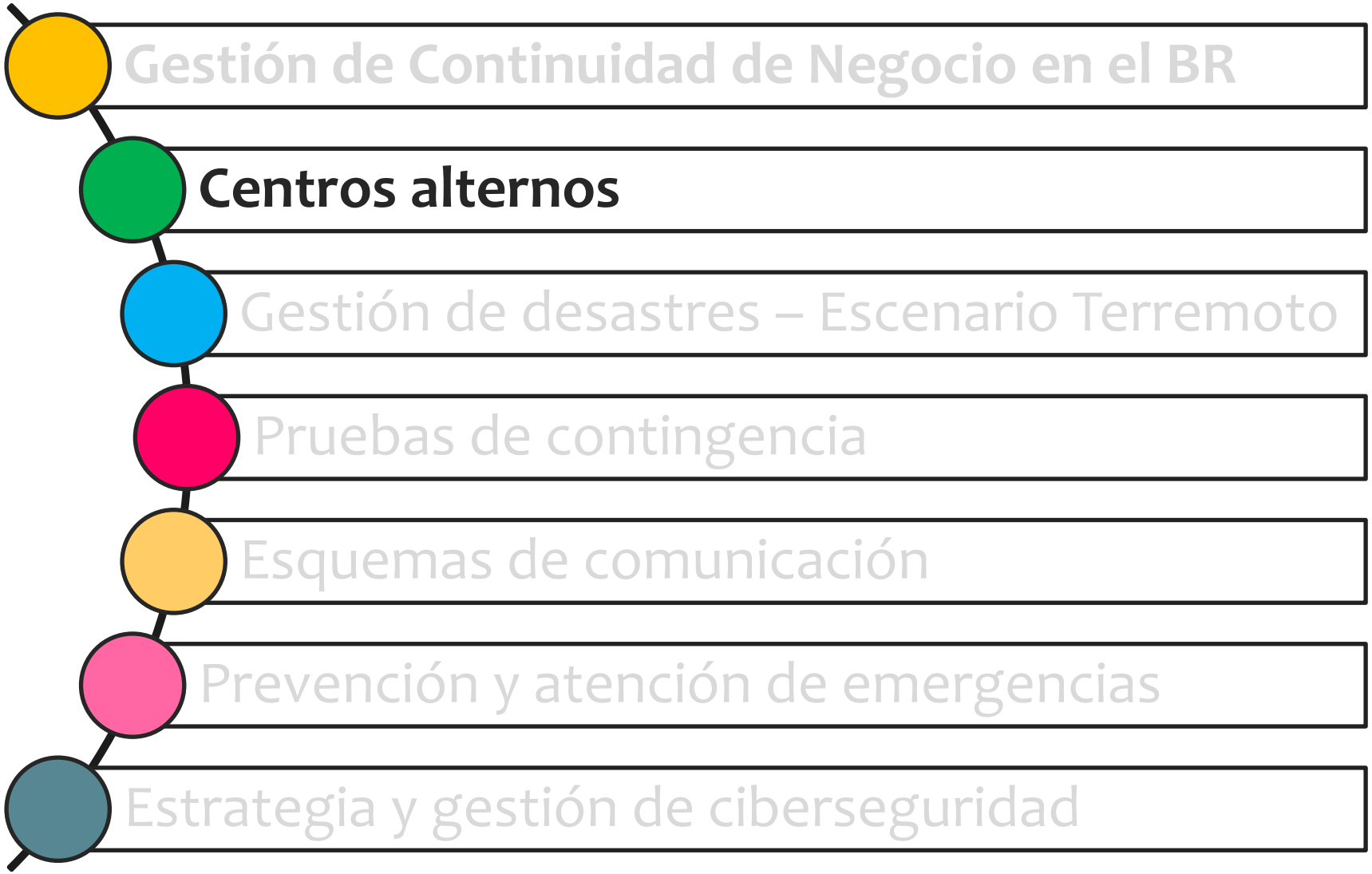
Agenda


Gestión de Continuidad de Negocio
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

Gestión de la Continuidad de Negocio



Agenda


Gestión de Continuidad de Negocio en el BR
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

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.

Nodos tecnológicos

Continuidad Tecnológica – principales componentes

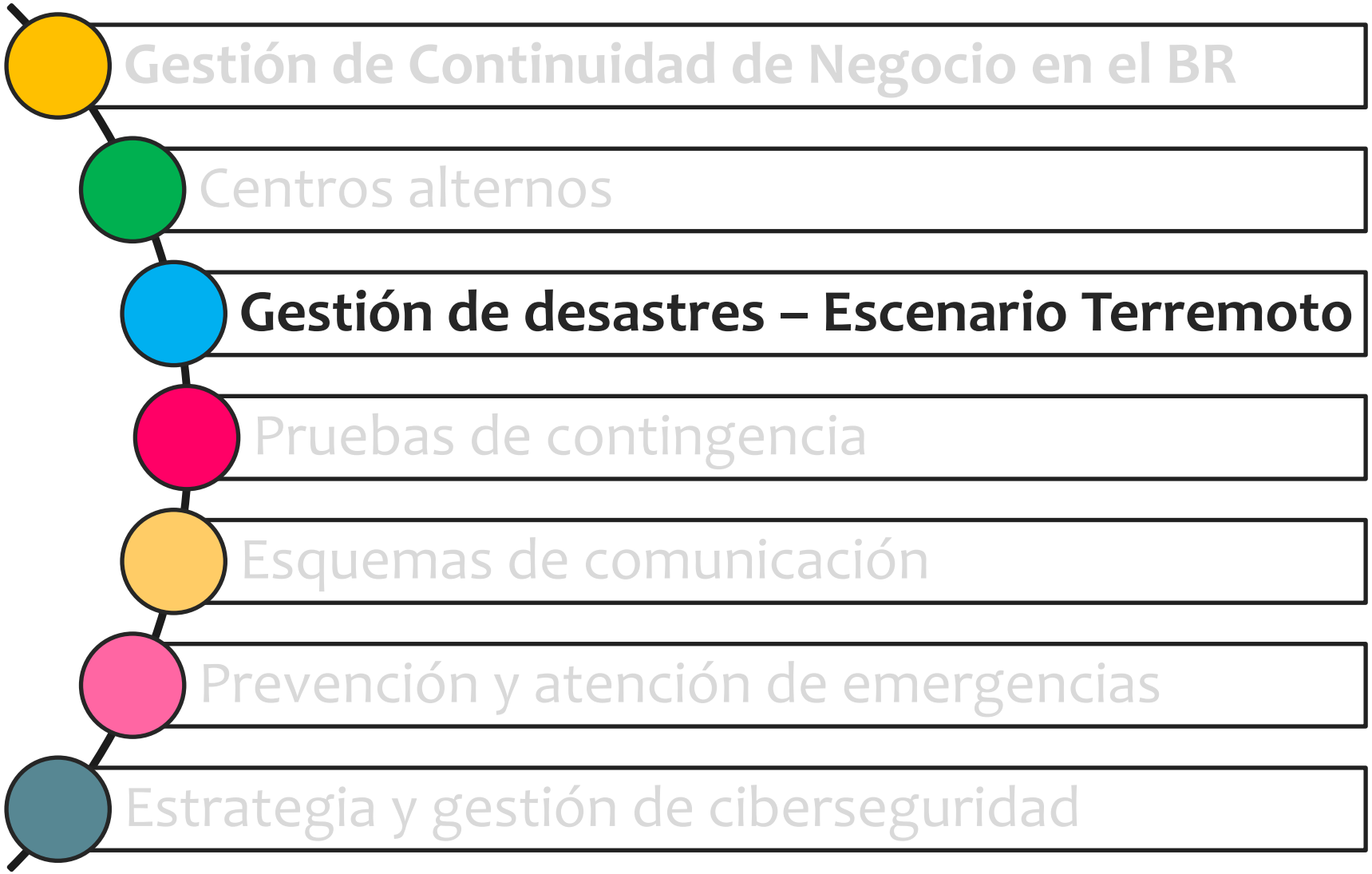
- Dos (2) nodos (primario y secundario) en Bogotá (Central de Efectivo y Ed. Ppal.) ~10 km. aprox.
  - Activos los dos nodos, cada servicio Activo – Activo, o Activo-Pasivo según su arquitectura / replicación sincrónica
  - RTO = entre 20 min. y 2 horas para los servicios críticos
  - RPO = 0 (sin pérdida de información en los datos de los servicios)

Un (1) tercer nodo 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

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

Agenda


Gestión de Continuidad de Negocio en el BR
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

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

- En caso de terremoto en Bogotá se cuenta con el **Plan de Provisión de Efectivo a EC 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

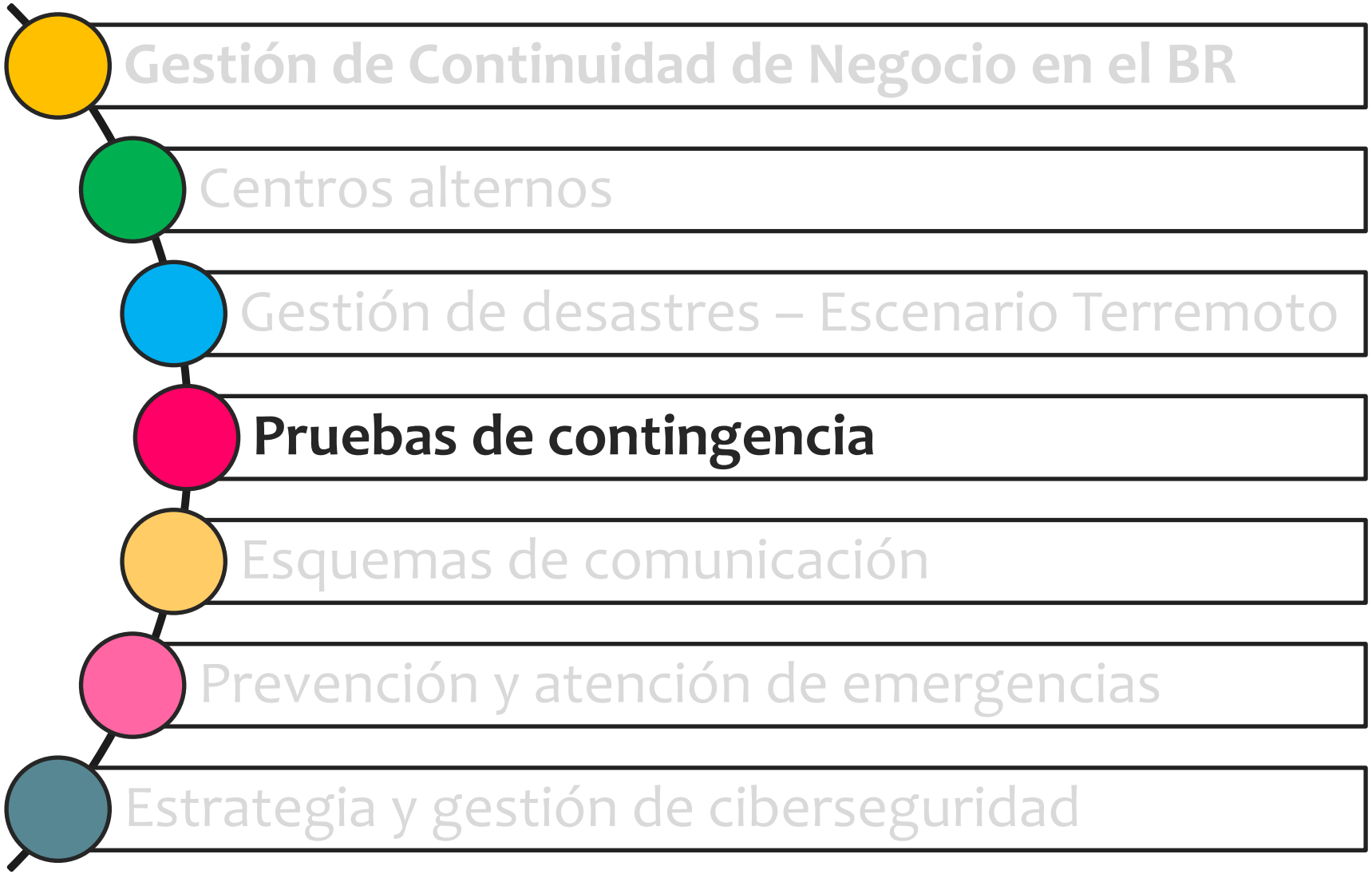
- **Ejercicios conjuntos** con Bancos, transportadoras de valores y proveedores de infraestructura (protocolo de comunicaciones con la RSSF, protocolo de crisis del MVD).

- Mecanismos de **comunicación ante desastres:** AtHoc Division of BlackBerry

Portal de Información de Desastres (PID)

018000
Línea de atención

Agenda


Gestión de Continuidad de Negocio en el BR
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

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 NO 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 hábil)**
  - Alcance: Simulación de pérdida del nodo secundario (edificio principal)
  - Participantes: Todas las entidades clientes del BR
  - Frecuencia: Semestral

Pruebas de contingencia

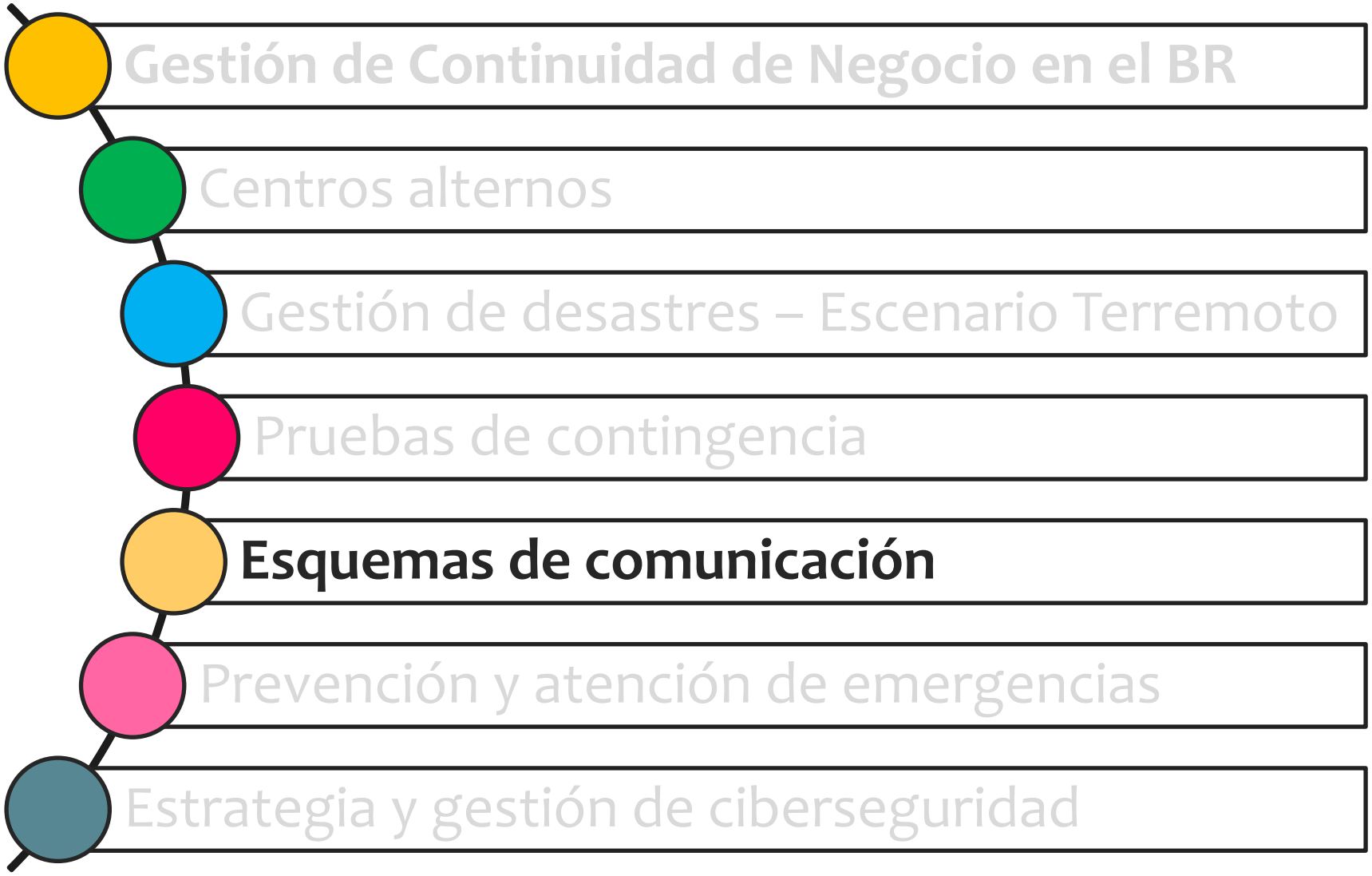
- **Prueba de Nodo Primario a Secundario (horario NO hábil)**
  - Alcance: simulación de pérdida del nodo primario (Central de Efectivo)
  - Participantes: Todas las entidades clientes del BR
  - Frecuencia: Semestral

- **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

- **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: Según

- **Cronograma de pruebas disponible en el sitio web del BR:**
  http://www.banrep.gov.co/es/continuidad/pruebas-contingencia

Agenda


Gestión de Continuidad de Negocio en el BR
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

Esquemas de comunicación de incidentes

- Correo electrónico a cuentas ContinuidadBR@entidad **indicando la no disponibilidad del servicio.**

- Mensaje en el sistema de audio-respuesta: 3431000 (línea de soporte).

- Correo electrónico indicando que el servicio ya se encuentra disponibles y la hora de inicio y fin del incidente.

Esquemas de comunicación - Contingencias

- Correo electrónico a cuentas ContinuidadBR@entidad **indicando los servicios que se encuentran en contingencia.**
- Mensaje en el sistema de audio-respuesta: 3431000 (línea de soporte),si es masivo.
- 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

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

ASUNTOS TECNOLÓGICOS

CAMBIOS

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,

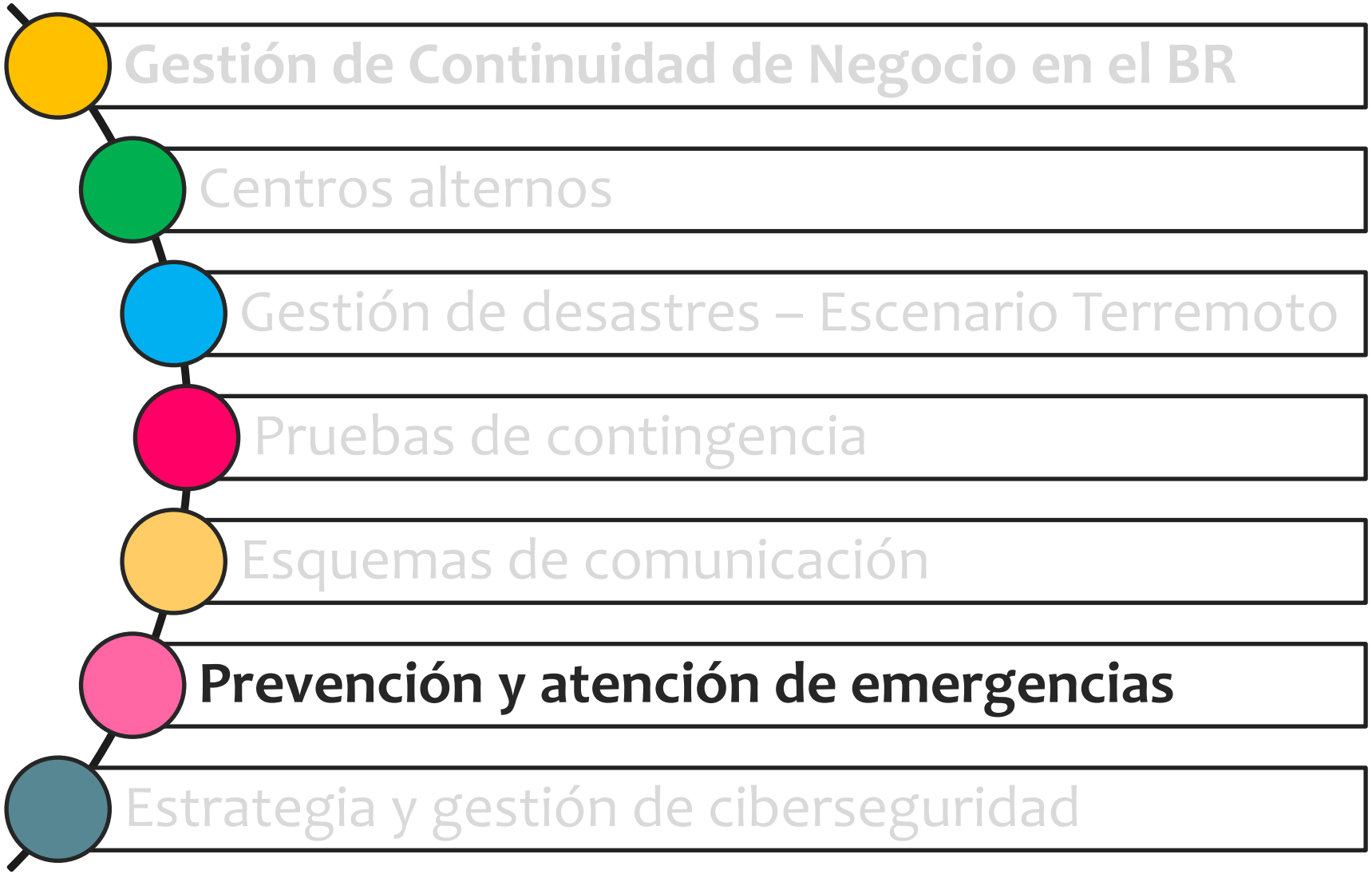
Departamento de Servicios de Tecnología Informática
Dirección General de Tecnología

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.

Agenda


Gestión de Continuidad de Negocio en el BR
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

Prevención y atención de emergencias: Principales componentes

- **Manuales**
  - Manuales de prevención y atención de emergencias por edificación a nivel nacional / estructura de gobierno.

- **Personas y capacitaciones**
  - Brigadas básicas en cada uno de los edificios.
  - Brigadistas de emergencia certificados.
  - Capacitaciones anuales.
  - Exámenes de aptitud por medio de valoración medica.

- **Simulacros**
  - Un (1) simulacro de evacuación anual por edificación

- **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

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

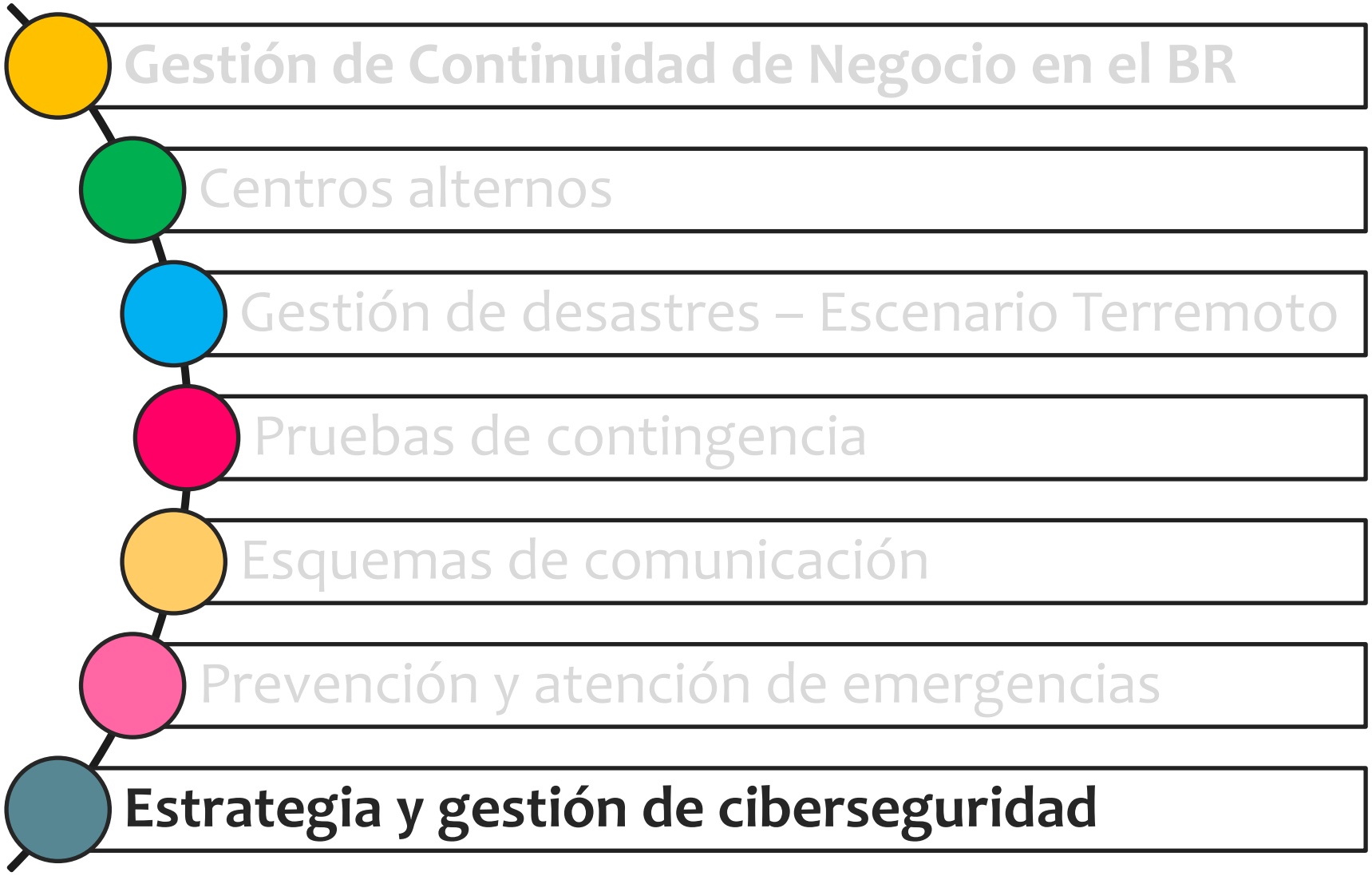
- **Elementos de seguridad**
  - Dotación para brigadistas de emergencia[1]
  - Paletas para las brigadas de evacuación
  - Pasamanos
  - Cintas antideslizantes
  - Lámparas de emergencia
  - Cintas fotoluminiscentes

- **Recursos de emergencia**
  - Botiquines
  - Silla de evacuación por escaleras
  - Desfibrilador externo automático
  - Camillas

- **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 Especifico de Respuesta – PER con el cuerpo oficial de Bomberos

1. Casco, overol, gafas, botas y chalecos

Agenda


Gestión de Continuidad de Negocio en el BR
Centros alternos
Gestión de desastres – Escenario Terremoto
Pruebas de contingencia
Esquemas de comunicación
Prevención y atención de emergencias
Estrategia y gestión de ciberseguridad

Estrategia y gestión de ciberseguridad

Marco de Ciberseguridad

DEFINICIÓN:

Basándose en el Cyber Security Framework del NIST, en el 2018 el Banco hizo una autoevaluación de sus capacidades para identificar sus activos (especialmente los críticos), protegerlos, detectar amenazas, responder ante eventos mayores y recuperarse ante un ciberataque. Como resultado, se definieron varias iniciativas, con el fin de buscar el mejoramiento continuo de la **postura de seguridad** y aumentar la **resiliencia**. Esta primera parte del ejercicio cerró en el Q4-2021.

SEGUIMIENTO:

- Trimestralmente, el comité de la Dirección de Tecnología revisa los indicadores asociados
- Semestralmente, el Comité de Riesgo hace el seguimiento al avance de las iniciativas.
- La auditoría interna revisa el avance de las iniciativas mediante reuniones regulares y evaluaciones directas. La auditoría externa evalúa niveles de madurez de procesos con chequeos aleatorios.
- En el 2022 se definirá un nuevo horizonte y se contará con la valoración del proceso por parte de un servicio externo.

Estrategia de Ciberseguridad – Postura

Para identificar la capacidad de defensa de la organización ante las amenazas cibernéticas, el Banco analiza su postura desde diferentes frentes:

Estrategia de Ciberseguridad – Ciber Resiliencia

El marco de ciberseguridad definido, además de identificar oportunidades de mejora en cinco las capacidades, también permite definir una estrategia de ciberseguridad enfocada principalmente en la **ciber resiliencia**.

Estrategia de ciberseguridad - Iniciativas

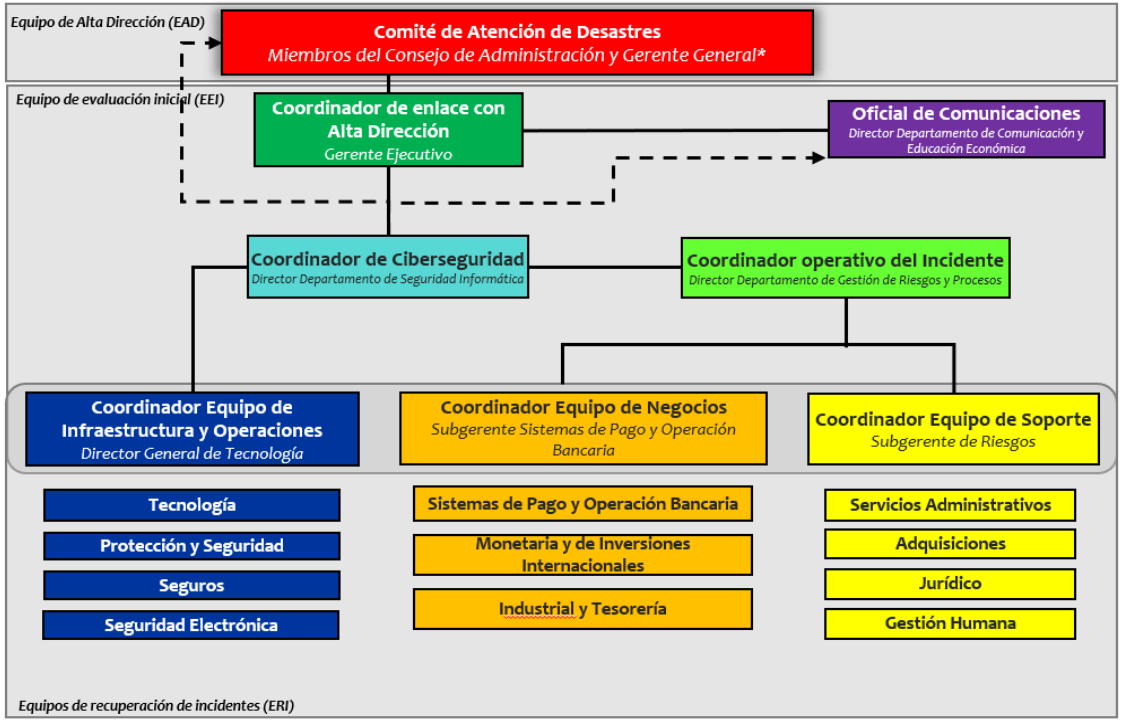
Acciones específicas que apoyan la estrategia son:

- Políticas de seguridad y ciberseguridad, adaptadas a las necesidades emergentes.
- Ejecución de campañas de concienciación generales y por grupos de interés.
- Ejecución de pruebas de EH y escaneo de vulnerabilidades sobre las plataformas internas y servicios externos.
- Ejecución de ejercicios de simulación de eventos mayores de seguridad y participación en ejercicios similares del sector para aprender lecciones. Desarrollo de playbooks con lecciones aprendidas.
- Centralización y operacionalización de inteligencia de amenazas con consumo de fuentes libres y pagas.
- Operacionalización de servicios tipo SOC para monitoreo continuo de eventos de seguridad
- Acceso a servicios tipo Retainer para apoyar la atención de incidentes de ciberseguridad de alto impacto y mejorar las capacidades de respuesta.
- Implementación de un nuevo SIEM que incluye analítica de comportamiento de usuarios y entidades (UEBA) para detectar anomalías para centralización de alertas de la premisa y la nube.
- Implementación de una plataforma SOAR (*Security Orchestration, Automation and Response*) para enriquecer las alertas y mejorar la eficiencia operativa.
- Implementación de una plataforma BAS (*Breach and Attack Simulation*) para validar la efectividad de los mecanismos implementados.

Estrategia de Ciberseguridad - Ciberdesastres

La ciber resiliencia está fundamentada en la adecuada preparación para atender eventos de desastre. Para ello se ha venido trabajando en el protocolo de gestión de desastres cibernéticos para los servicios críticos del Banco:

- Definición de las joyas de la corona por la Alta Gerencia
- Ajuste del gobierno de gestión de desastres ante un evento de desastre cibernético
- Ajuste al plan de comunicaciones
- Pre-autorizaciones para detener total o parcialmente servicios, según la valoración del desastre
- Playbooks para responder ante eventos de desastre asociados a malware avanzado, fuga de información o denegación de servicio



En general, el Banco priorizará la integridad de los datos sobre la disponibilidad del servicio en los sistemas y plataformas críticas si llegase a ser requerido, y se reservará el derecho a interrumpir la operación mientras son llevadas a cabo investigaciones para asegurar la integridad y la calidad de los mismos.

Reporte de incidentes de ciberseguridad CE007-CE033

El Banco ha establecido el uso del buzón, del protocolo TLP de etiquetado y de la taxonomía en el marco del procedimiento interno de gestión de incidentes de seguridad y ciberseguridad para documentar los reportes a la SFC, si el incidente lo amerita.

El Banco reporta trimestralmente los indicadores solicitados por la SFC en la CE-033.

Gracias!