



CKC

Logramos que suceda

El Paradigma del DRP vs Continuidad Tecnológica



¿Por qué estamos aquí?

Desastres Naturales



Pandemia/Manifestaciones/Huelgas



Tecnológicas/Seguridad

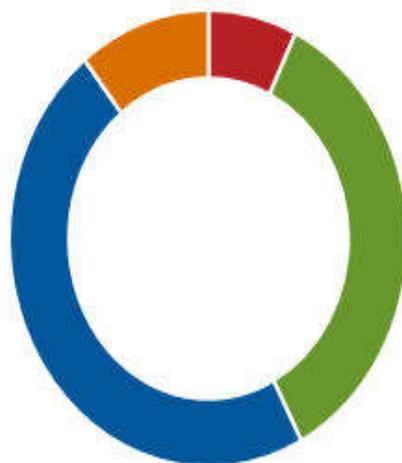




Impactos globales

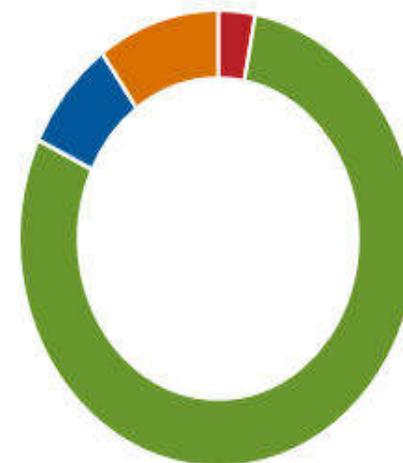
Percentage distribution for relevant natural loss events worldwide 2017

Number of events:
736



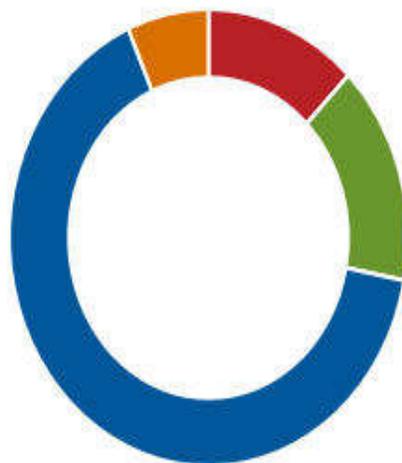
- 7.2 %
- 35.1 %
- 47 %
- 10.7 %

Overall losses:
US\$ 340bn



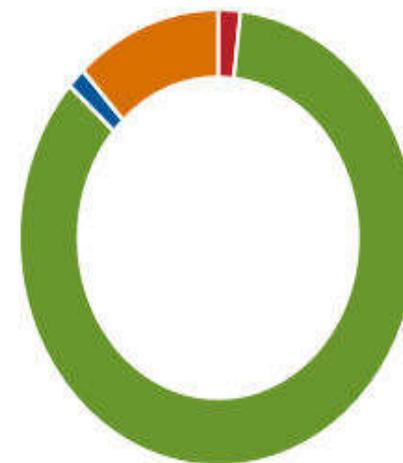
- 3 %
- 79.1 %
- 8 %
- 9.9 %

Fatalities:
9,947



- 12.4 %
- 15.6 %
- 65.4 %
- 6.6 %

Insured losses:
US\$ 138bn



- 1.8 %
- 84.8 %
- 1.5 %
- 11.9 %

● Geophysical events ● Meteorological events ● Hydrological events ● Climatological events



Principales Desafíos

- Diversidad de Regulaciones que agregan complejidad a las operaciones
- Baja tolerancia a discontinuidad operativa



- Necesidad de mejores niveles de servicio
- Madurez del Modelo operativo de TI



Pérdidas Asociadas a la Continuidad

Pérdidas de Utilidad

- Pérdidas Directas
- Pagos Compensatorios
- Pérdidas Futuras
- Pérdidas de Inversión

Gastos Extra

- Costo de Recuperación
- Gastos de horas extras
- Riesgo de Fraude
- Riesgo de errores
- Viáticos
- Empleados temporales

Multas

- Contractuales
- Regulatorias
- Legales

Pérdidas de Productividad

- Nómina Impactada
- Rentas

Recuperación retrasada

- Facturación perdida
- Descuentos

Reputación dañada

- Clientes, proveedores, socios, bancos, mercados financieros, competencia.
- Historial crediticio





¿Qué busca el negocio?

Resiliencia

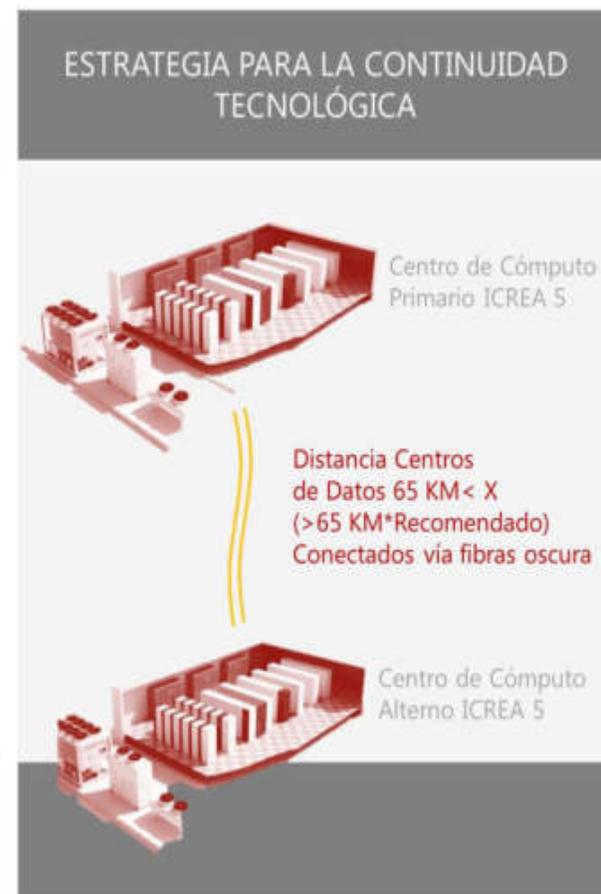
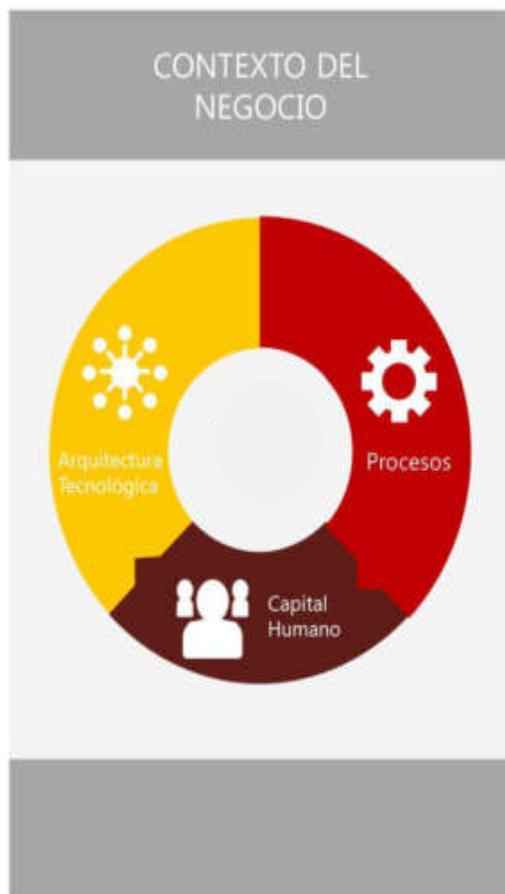
“Capacidad de un sistema de recuperarse al ser afectado por una crisis de cualquier tipo u origen”





Visión Sistémica del Negocio hacia la Continuidad

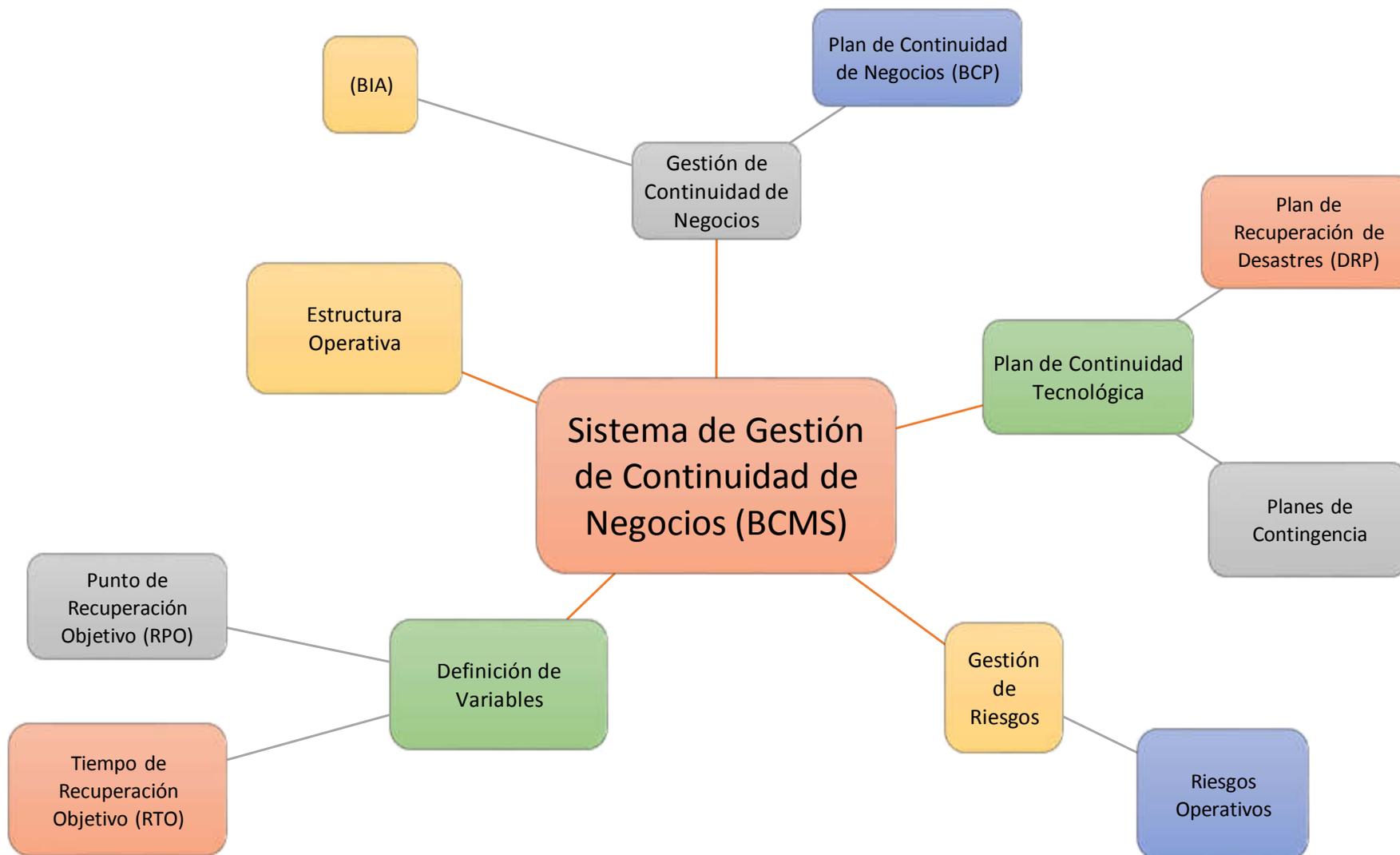
Estrategia



Implementación

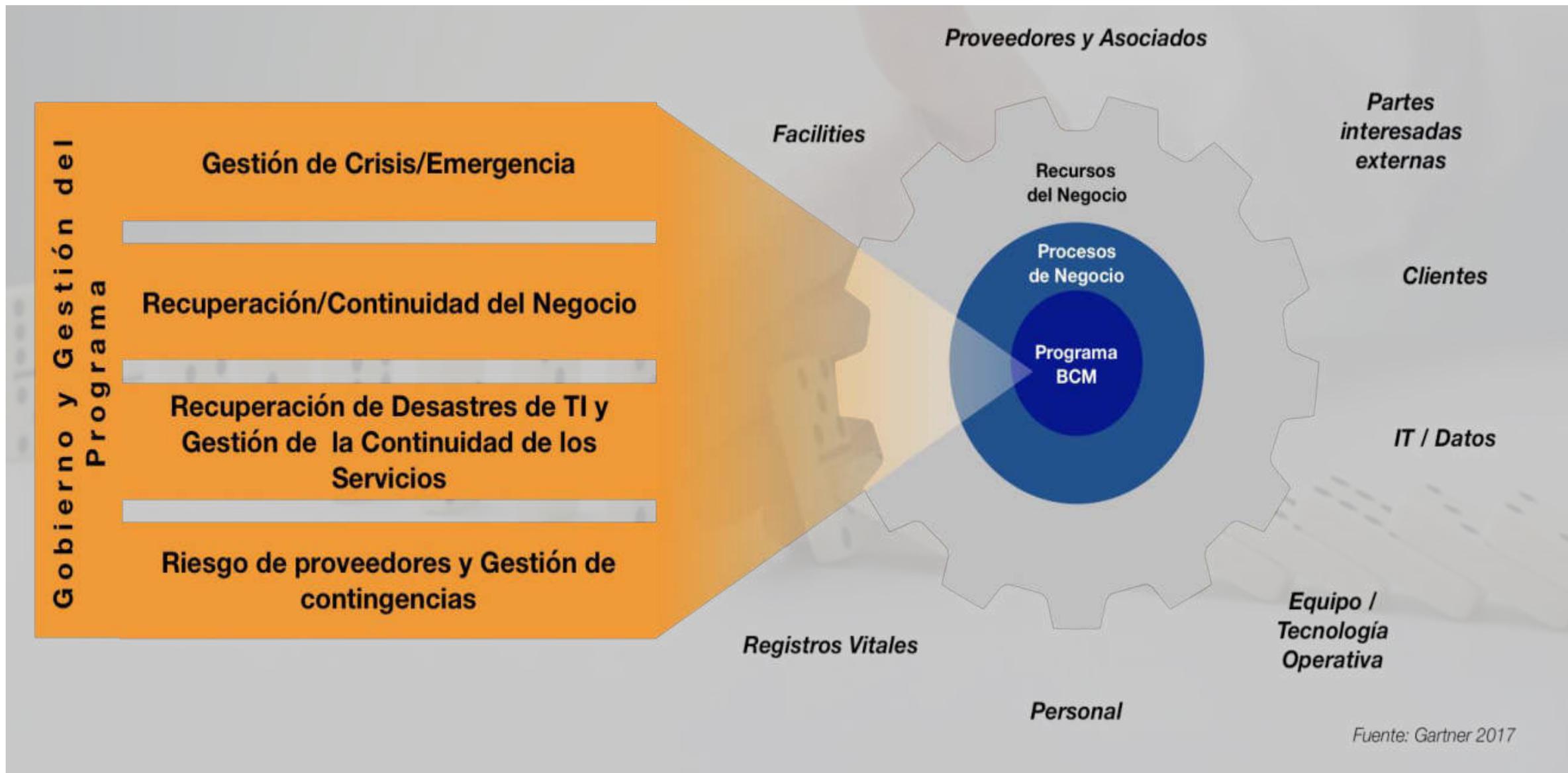


Componentes de la Continuidad





Modelo de Gobierno





Responsabilidades

El BCM es una iniciativa de toda la organización

Gobernar y administrar un programa de BCM es una iniciativa de toda la empresa. El personal que administra las operaciones diarias es el mismo que el responsable de realizar las actividades del programa BCM.

La siguiente tabla describe las relaciones de informes de mejores prácticas para cada disciplina.



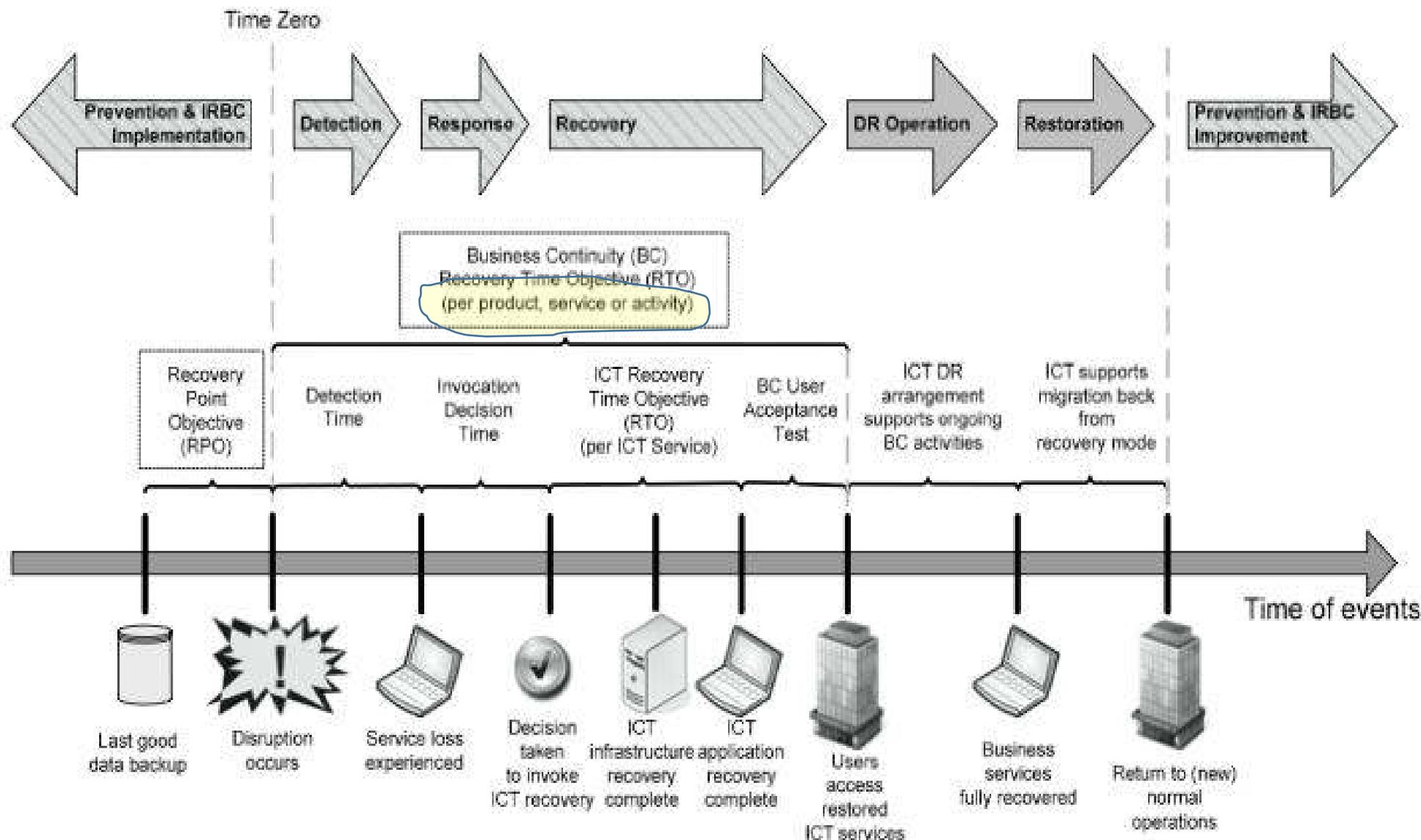
| Disciplina del Programa BCM | Mejores Practicas de Responsabilidad directa para la gestión |
|--|--|
| Gobierno y Gestión del Programa BCM | Dirección / Responsable del Riesgo Operacional Supervisión del Comité de Dirección BCM |
| Manejo de Crisis/Incidentes | Ejecutivos de Alta Gerencia Office Manager BCM program office manager como facilitador |
| Recuperación del Negocio | Oficial del programa de BCM, en conjunto con las unidades del negocio |
| Recuperación de Desastres de TI y Gestión de la Continuidad de los Servicios | CIO / Director de Sistemas |
| Riesgo de proveedores y Gestión de contingencias | BCM program office, en conjunto con las unidades de adquisición y de negocio |



DRP vs Continuidad Tecnológica

Recuperación

- El proceso de recuperación a un estado interno
- Se activa



Plan de Continuidad

- Es la capacidad de prevenir en servicio



Cuestiones Clave

Procesos clave a soportar

- ¿Cuáles son los procesos de negocio y subprocessos clave que requieren un aseguramiento en su continuidad desde su habilitación tecnológica?
- ¿Qué información es necesario mantener operativa?
- ¿Cuáles son los requerimientos mínimos de operación a asegurar?
- ¿Cuál es el impacto asociado de no operar esos procesos?

Opciones estratégicas de continuidad

- ¿Qué infraestructura tecnológica soporta a los procesos clave y requiere de continuidad?
- ¿Qué indicadores pueden ser adoptados para el monitoreo y prevención de eventos de riesgo de continuidad?
- ¿Qué modelo operativo de TI, infraestructura organizacional y capacidades deben de ser desarrolladas para asegurar la continuidad?
- ¿Qué opciones de tercerización pueden contribuir al aseguramiento de la continuidad tecnológica?
- ¿Dónde se reanudará la operación de los procesos críticos?

Implantación del plan

- ¿Cuál es el mejor esquema de implantación del plan de continuidad tecnológica?
- ¿Qué funciones y responsabilidades clave deben de ser modificadas/agregadas para mantener vigente el plan de continuidad tecnológica?
- ¿Cómo podemos medir el éxito del plan de continuidad tecnológica sin que entre en operación?



Errores mas Comunes

- No identificar los componentes habilitadores críticos
- No considerar a todas las partes interesadas ni los recursos necesarios
- Personal no capacitado ni concientizado en el tema
- Pensar “a mi no me va a pasar” o “no lo necesito”
- Pensar que continuidad de TI es “solo el DRP”
- Planes muy generales o considerando solo el “worst case”
- Pruebas y ejercicios no ejecutados o mal planificados



Principios

POR COMPONENTE Y GLOBAL





Alineación Estratégica

Estrategias Negocio

Estrategias Tecnológicas

Planes de Contingencia

Oficinas Alternas de Operación

HOT SITE Activo-Activo

WARM SITE Activo-Pasivo

COLD SITE Activo-Pasivo

1. Aplicaciones críticas
2. Comunicaciones críticas
3. Punto de quiebre DRP vs Plan(es) de Contingencia

Recuperación de Desastres

Centros de Datos de Operación

HOT SITE Activo-Activo

WARM SITE Activo-Pasivo

COLD SITE Activo-Pasivo

Sala Cómputo

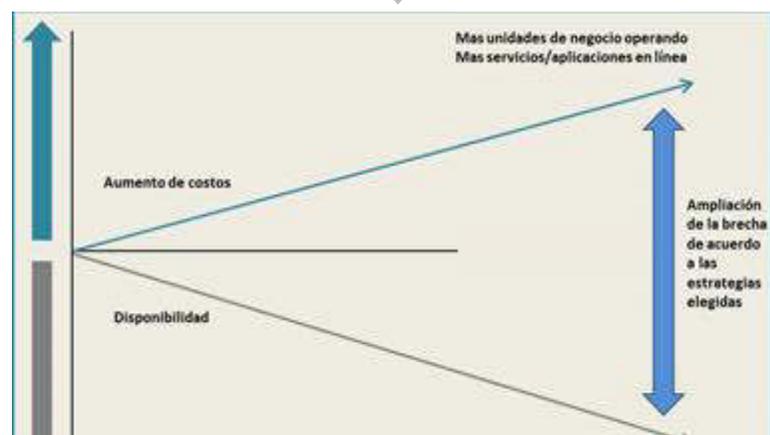
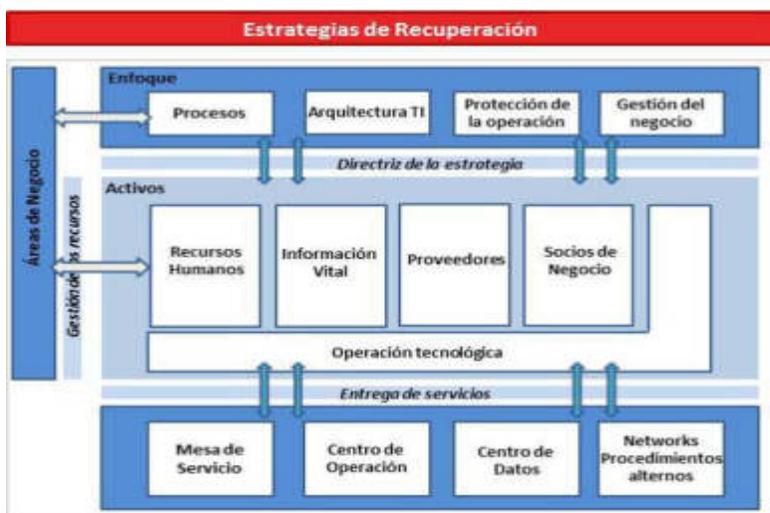
1. Propio
2. Arrendado

Servidores

1. Físicos
2. Virtuales

Aplicaciones

1. Activo-Activo
2. Activo-Pasivo





PREGUNTAS Y RESPUESTAS



CKC

Logramos que suceda

GRACIAS

Carlos Kornhauser
carlos.kornhauser@ckc.com.mx